КОД безопасности

Средство защиты информации

Secret Net Studio – C

Руководство администратора

Настройка и эксплуатация

RU.88338853.501400.002 91 2

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

AD	Active Directory
ARP	Address Resolution Protocol
BSOD	Blue Screen of Death
CRC	Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DNS	Domain Name System
FAT	File Allocation Table
HTTP	Hypertext Transfer Protocol
ICMP	Internet Comtrol Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long File Name
MBR	Master Boot Record
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
RTF	Rich Text Format
SD	Secure Digital
SID	Security Identifier
SMB	Server Message Block
TCP	Transmission Control Protocol
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
АРМ	Автоматизированное рабочее место
БД	База данных
БС	Безопасная среда
ДС	Доверенная среда
ЗПС	Замкнутая программная среда
ИБП	Источник бесперебойного питания
КС	Контрольная сумма
КЦ	Контроль целостности
ЛБД	Локальная база данных
МД	Модель данных
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РС	Рабочая станция

СБ	Сервер безопасности
СЗИ	Средство или система защиты информации
СОВ	Система обнаружения вторжений
СПС	Состояние программной среды
ЦБД	Центральная база данных
ЦУ	Центра управления
ЭЦП	Электронная цифровая подпись

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio – C" RU.88338853.501400.002 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для настройки и управления механизмами защиты изделия:

- базовая защита:
  - защита входа в систему (локальная аутентификация, персональные идентификаторы);
  - защита терминальных подключений;
  - самозащита;
  - теневое копирование;
  - локальный аудит (журналы, оповещение о тревогах);
  - паспорт ПО;
- локальная защита:
  - контроль устройств;
  - контроль печати;
  - контроль целостности ресурсов;
  - замкнутая программная среда;
  - полномочное управление доступом;
  - дискреционное управление доступом к ресурсам файловой системы;
  - защита информации на локальных дисках;
  - шифрование данных на дисках;
  - шифрование данных в криптоконтейнерах;
  - затирание удаляемой информации;
- сетевая защита:
  - межсетевой экран;
  - авторизация сетевых соединений;
- доверенная среда;
- безопасная среда.

Перед изучением данного руководства рекомендуется ознакомиться с общими сведениями о Secret Net Studio, изложенными в документе [**1**].

Условные обозначения

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

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний.

Другие источники информации

Сайт в интернете. 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
Настройка локальной аутентификации

Управление режимами механизма защиты входа в систему

Действие механизма защиты входа в систему регулируется рядом параметров, которые можно настроить централизованно и локально.

При централизованном управлении имеется возможность настраивать параметры защиты входа в систему для клиентов с Secret Net Studio и с Secret Net LSP. Совместное управление осуществляется только на уровне групповых политик серверов безопасности, доменов безопасности и организационных подразделений.

К компьютерам с Secret Net LSP применимы не все имеющиеся параметры. Ограничения можно определить по пиктограммам, которые по умолчанию отображаются для каждого параметра и указывают на применимость параметра к разным клиентам:

-  — параметр применим для клиента с Secret Net Studio;
-  — параметр применим для клиента с Secret Net LSP.

Пояснение. Также имеются особенности применения параметров в зависимости от используемого на компьютере дистрибутива Linux. Подробная информация о таких особенностях приведена в документации на СЗИ Secret Net LSP.

Совет. Отключить или включить отображение пиктограмм можно в настройках Центра управления. Для этого выполните следующие действия:

- в нижней части панели навигации нажмите кнопку "Настройки";
- выберите ссылку "Настройки центра управления";
- в появившемся диалоге перейдите к группе параметров "Политики";
- удалите или установите отметку в поле "Показывать поддерживаемую платформу для политик".

Ниже приводится описание процедуры централизованной настройки параметров на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки режимов механизма защиты входа:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Вход в систему".
3. Настройте параметры, приведенные в таблице ниже.

Максимальный период неактивности до блокировки экрана
Устанавливает максимально возможный период неактивности, после которого компьютер автоматически блокируется средствами системы защиты. В целях безопасности при продолжительном бездействии пользователя компьютер должен блокироваться. Блокировка по истечении заданного периода неактивности осуществляется средствами системы защиты. Пользователи с помощью стандартных средств операционной системы могут указать для компьютера другой период включения блокировки (заставки), но этот период не может быть больше значения данного параметра. В противном случае параметр ОС не будет действовать. Если установлено значение "0" — блокировка средствами системы защиты не осуществляется. Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP
Запрет вторичного входа в систему
Если режим включен, блокируется запуск команд и сетевых подключений с вводом учетных данных пользователя, не выполнившего интерактивный вход в систему. После включения режима дополнительно рекомендуется исключить возможность использования ранее сохраненных учетных данных. Для этого включите действие стандартного параметра безопасности ОС Windows "Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности" (название параметра может незначительно отличаться в зависимости от версии ОС). Параметр применим только для компьютеров с Secret Net Studio
Запрет смены пользователя без перезагрузки
Если режим включен, то для смены пользователя или завершения сеанса пользователя необходима перезагрузка компьютера. Если при включенном режиме произошла блокировка компьютера, то необходимо выполнить перезагрузку компьютера администратору для снятия блокировки и далее пользователю для последующего входа в систему. При снятии блокировки централизованно с использованием Центра управления перезагрузка компьютера не требуется. Не следует включать данный режим на терминальном сервере, так как это приведет к невозможности работы клиентов с сервером. Параметр применим для компьютеров с Secret Net Studio (версии 8.8 и выше)
Реакция на изъятие идентификатора
Не блокировать — при изъятии идентификатора из считывающего устройства блокировка компьютера не выполняется. **Блокировать станцию при изъятии USB-идентификатора** — выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора на базе USB-ключа или смарт-карты, использованного для идентификации пользователя в системе защиты (например, eToken). **Блокировать станцию при изъятии любого идентификатора** — выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора любого типа из числа поддерживаемых системой защиты для идентификации пользователей (iButton, eToken и др.). Блокировка при изъятии идентификатора применяется, если идентификатор активирован средствами системы защиты и пользователь предъявил этот идентификатор для входа в систему. Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP
Количество неудачных попыток аутентификации
Устанавливает ограничение на количество неудачных попыток входа в систему при включенном режиме усиленной аутентификации по паролю. При достижении ограничения: • на компьютерах с Secret Net Studio компьютер блокируется согласно политике "Время блокировки при достижении количества неудачных попыток аутентификации", и вход разрешается только администратору; • на компьютерах с Secret Net LSP учетная запись пользователя блокируется в соответствии с политикой "Время блокировки при достижении количества неудачных попыток аутентификации". Вход под учетной записью другого пользователя возможен. Если установлено значение "0" — ограничение не действует. Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP

Время блокировки при достижении количества неудачных попыток аутентификации

Определяет продолжительность блокировки компьютера при достижении ограничения количества неудачных попыток аутентификации:

- на компьютерах с Secret Net Studio компьютер блокируется на заданный промежуток времени, по истечении которого блокировка автоматически снимается и пользователь может выполнить вход в систему. До истечения заданного промежутка времени снять блокировку может только администратор. При значении "0" компьютер блокируется бессрочно и вход разрешается только администратору;
- на компьютерах с Secret Net LSP учетная запись пользователя блокируется на заданный промежуток времени, по истечении которого блокировка автоматически снимается и пользователь может выполнить вход в систему. До истечения заданного промежутка времени снять блокировку с учетной записи пользователя может только администратор. При значении "0" учетная запись блокируется бессрочно.

Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP

Разрешить интерактивный вход только доменным пользователям

Если режим включен, интерактивно в систему могут войти только пользователи, зарегистрированные в домене. Интерактивный вход в систему локальных пользователей (включая локальных администраторов) запрещен.

Параметр отсутствует при локальной настройке на компьютере с установленным клиентом в автономном режиме функционирования.

Параметр применим только для компьютеров с Secret Net Studio

Режим идентификации пользователя

По имени. Для входа в систему пользователь должен ввести свои учетные данные, используя только стандартные средства ОС.

Смешанный. Для входа в систему пользователь может предъявить идентификатор, зарегистрированный в системе защиты, или ввести свои учетные данные, используя стандартные средства ОС.

Только по идентификатору. Для входа в систему пользователь должен предъявить идентификатор, зарегистрированный в системе защиты. Пользователи, не имеющие персональных идентификаторов, войти в систему не смогут. В Secret Net Studio администратор может войти в систему без предъявления идентификатора только в административном режиме (см. стр.**19**).

Особенности:

- В режимах входа "По имени" и "Смешанный" допускается работа с USB-ключами и смарт-картами средствами ОС (например, см. документацию на ОС Windows). В режиме "Только по идентификатору" используются персональные идентификаторы, активированные средствами системы защиты, но не ОС.
- При использовании учетной записи Microsoft в ОС Windows 8 и Windows 10 вход в систему по идентификатору доступен только на компьютерах, включенных в домен.
- Если для двух защищаемых компьютеров выбраны разные режимы аутентификации, правила межсетевого экрана для аутентифицированных пользователей между ними не сработают (см. стр.**210**).

Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP

Режим аутентификации пользователя

Стандартная аутентификация — при входе пользователя выполняется только стандартная аутентификация ОС.

Усиленная аутентификация по паролю — при входе пользователя, помимо стандартной аутентификации ОС, дополнительно выполняется аутентификация по паролю пользователя средствами системы Secret Net Studio. В этом режиме пользователи, пароль которых не был сохранен в базе данных системы Secret Net Studio, не смогут войти в систему (администратор может разрешить пользователю разовый вход для сохранения пароля, включив параметр "Доверять парольной аутентификации Windows при следующем входе в систему" в диалоге настройки свойств пользователя). Для выполнения операций с пользователями в программе "Управление пользователями" будет необходимо ставить отметку в поле "Синхронизировать данные пользователя на сервере аутентификации" при выполнении каждой операции либо поставить отметку в поле "Доверять аутентификации Windows" в Центре управления.

Вход в систему разрешается при совпадении пароля с сохраненным значением. Если включен режим "Регистрировать неверные аутентификационные данные", неправильно введенный пароль сохраняется в журнале Secret Net Studio в виде зашифрованной последовательности символов.

Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP

Парольная политика
Определяет действующие требования к паролям пользователей при включенном режиме усиленной аутентификации по паролю. Требования совпадают с заданными параметрами политики паролей Windows, если включен режим "Брать значения из парольной политики Windows". В этом случае значения парольной политики для компьютеров с Secret Net LSP останутся заданными по умолчанию. При необходимости могут применяться особые требования для паролей, сохраняемых в базе данных системы защиты (независимо от заданных параметров политики паролей в ОС). Для этого выберите режим "Задать свои значения" и настройте требования, аналогичные стандартным параметрам политики паролей ОС "Минимальная длина пароля", "Срок действия пароля", "Сложность пароля", "Минимальное число измененных символов нового пароля". При этом на компьютерах в конечном итоге будут применяться наиболее "строгие" параметры из тех, которые заданы в политиках системы защиты и ОС. Параметры применимы для компьютеров с Secret Net Studio и с Secret Net LSP. Параметр "Минимальное число измененных символов нового пароля" применим для компьютеров с Secret Net Studio версии 8.8 и выше
Оповещение пользователя
Оповещение пользователя о последнем успешном входе в систему — после успешного входа пользователя в систему отображается информационное сообщение о последнем успешном входе этого пользователя. Например, на компьютерах с Secret Net Studio над системной областью панели задач Windows отображается сообщение со следующей информацией: • дата и время предыдущего входа; • количество неудачных попыток входа с момента последнего успешного входа. В случае отсутствия информации о предыдущем успешном входе отображается сообщение "Данные о предыдущем входе пользователя отсутствуют". На компьютерах с Secret Net Studio сообщение с информацией о последнем успешном входе может не отобразиться в случае появления двух и более других информационных сообщений. Параметр применим для компьютеров с Secret Net Studio и с Secret Net LSP. **Предупреждение пользователя о мерах защиты информации до входа в систему** — до входа пользователя в систему на экране блокировки отображается информационное сообщение о реализованных в системе мерах защиты информации. Выполняя вход в систему, пользователь соглашается с необходимостью соблюдения правил и ограничений на работу с информацией. Параметр применим только для компьютеров с Secret Net Studio

4. Настройте регистрацию событий, относящихся к работе механизма. Для перехода к соответствующей группе параметров регистрации используйте ссылку "Аудит" в правой части заголовка группы.
5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Разрешение разового входа при усиленной аутентификации по паролю

Если используется режим усиленной аутентификации пользователей по паролю, при входе пользователя дополнительно выполняется аутентификация по его паролю средствами Secret Net Studio. Для этого информация о пароле пользователя должна быть сохранена в базе данных Secret Net Studio. Сохранение этой информации может выполняться при первом успешном входе пользователя в систему, при смене пароля самим пользователем, а также при смене его пароля администратором.

На клиенте Secret Net Studio, функционирующем в автономном режиме, для пользователей доступен параметр "Доверять парольной аутентификации Windows при следующем входе в систему", позволяющий пользователю после включения режима усиленной аутентификации выполнить разовый вход в систему с сохранением информации о пароле в базе данных Secret Net Studio. После этого разрешение автоматически отключается, и для пользователя в полном объеме будет действовать режим усиленной аутентификации по паролю. При создании пользователей в программе управления пользователями данный параметр включается по умолчанию. Перед включением режима усиленной аутентификации пользователей по паролю рекомендуется средствами этой программы проверить и включить данный параметр для тех учетных записей пользователей, у которых он отключен (см. инструкцию ниже).

На клиенте Secret Net Studio, функционирующем в сетевом режиме, для доменных пользователей усиленная аутентификация осуществляется через сервер аутентификации Secret Net Studio. Доверие к парольной аутентификации Windows при первом входе пользователя регулируется настройками домена безопасности (Центр управления, группа параметров "Аутентификация Windows", параметр "Доверять парольной аутентификации Windows при первом входе в систему"). Если данная настройка включена и на клиенте выполняется первичный вход при включенной политике усиленной аутентификации – информация о пользователе будет сохранена в базу данных сервера аутентификации. В дальнейшем при отключении параметра "Доверять парольной аутентификации Windows при первом входе в систему" на сервере безопасности для пользователя в полном объеме будет действовать режим усиленной аутентификации по паролю.

Пояснение. В сетевом режиме функционирования в программе управления пользователями для доменных пользователей параметр "Доверять парольной аутентификации Windows при следующем входе в систему" выключен и недоступен для изменения.

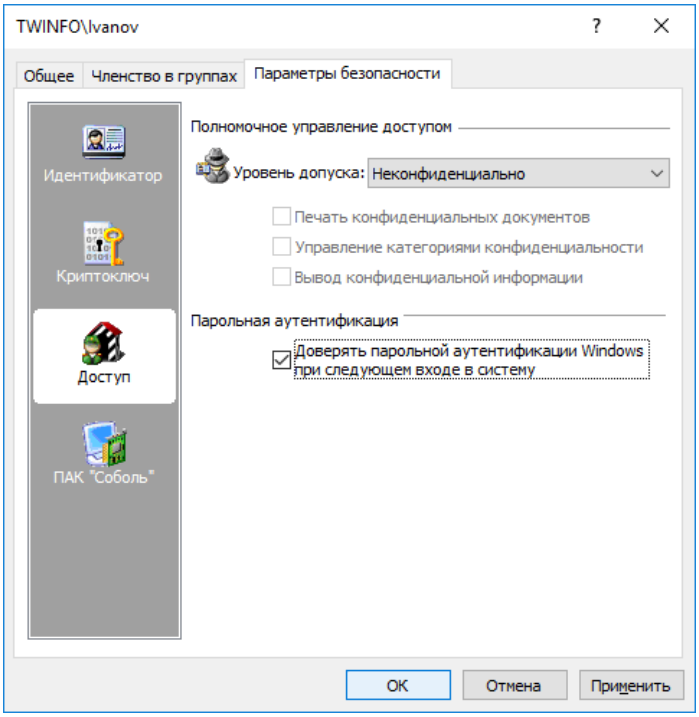
Информация о доменном пользователе может быть добавлена в базу данных сервера аутентификации в программе управления пользователями при создании пользователя, смене пароля существующего пользователя (параметр "Синхронизировать данные пользователя на сервере аутентификации") и при вызове команды "Синхронизировать с системой защиты" в контекстном меню пользователя.

Пояснение. Для удаления пользователя из базы данных сервера аутентификации установите параметр "Синхронизировать данные пользователя на сервере аутентификации" при удалении этого пользователя в программе управления пользователями.

Для локальных пользователей действуют те же правила что и для пользователей в автономном режиме функционирования.

Для разрешения разового входа пользователя в систему с Secret Net Studio в автономном режиме:

1. Запустите программу управления пользователями (см. стр.**270**).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. В панели выбора групп параметров выберите группу "Доступ".



4. Установите отметку в поле "Доверять парольной аутентификации Windows при следующем входе в систему".
5. Нажмите кнопку "OK".

Функциональный контроль

Функциональный контроль — это механизм самоконтроля системы защиты на предмет корректного функционирования ключевых подсистем Secret Net Studio. Если хотя бы одна из подсистем защиты в ходе функционального контроля не демонстрирует свою корректную работу, то:

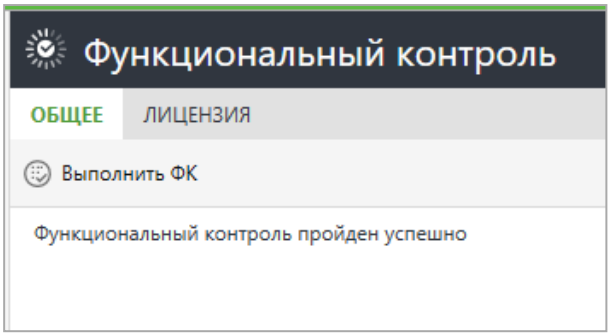
- вход непривилегированного пользователя в систему блокируется, вход доступен только администратору;
- администратор получает уведомление о нарушении функционального контроля;
- в журнале Secret Net Studio регистрируется событие о попытке несанкционированного доступа.

Инициализация защитных подсистем и их функциональный контроль выполняются во время загрузки компьютера перед входом пользователя. Вход пользователя в систему разрешается, если все проверки пройдены успешно.

Функциональный контроль можно выполнить в процессе работы на компьютере в централизованном и локальном режимах управления.

Для проведения функционального контроля:

1. В Центре управления или Локальном центре управления откройте панель "Компьютеры" и выберите вкладку "Состояние" для нужного компьютера.
2. Выберите плитку "Функциональный контроль". Справа отобразится блок с подробной информацией о механизме.



3. Нажмите кнопку "Выполнить ФК".

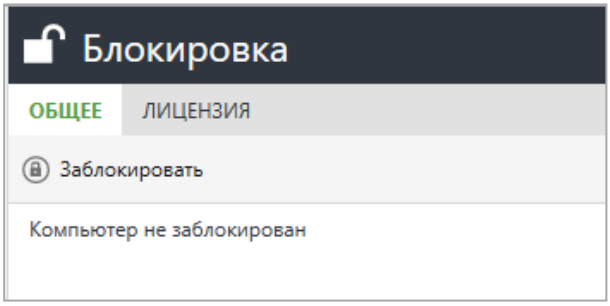
   При успешном прохождении процедуры отобразится сообщение "Функциональный контроль пройден успешно".

Блокировка рабочей станции

При определенных событиях системы защиты рабочая станция может быть заблокирована. Также администратор может заблокировать или разблокировать компьютер средствами Secret Net Studio централизованно или локально. В случае блокировки вход непривилегированного пользователя запрещается. При разблокировке ограничения на вход снимаются.

Для блокировки/разблокировки рабочей станции:

1. В Центре управления или Локальном центре управления откройте панель "Компьютеры" и выберите вкладку "Состояние" для нужного компьютера.
2. Выберите плитку "Блокировка". Справа отобразится блок с информацией о состоянии компьютера.



3. Нажмите кнопку "Заблокировать"/"Разблокировать".

   Появится окно с запросом на подтверждение действия.
4. Нажмите кнопку "Да".

Вход в систему в штатном режиме

При штатном функционировании системы Secret Net Studio вход любого пользователя компьютера, включая администратора, должен выполняться по одинаковым правилам, установленным соответствующими механизмами защиты.

Пояснение. Порядок входа пользователя в систему при функционировании Secret Net Studio приведен в документе [3].

При включенных параметрах оповещения пользователя до входа (на экране блокировки) или после входа (над системной областью панели задач) в систему могут отобразиться информационные сообщения (см. стр.15).

Внимание! При появлении на экране блокировки сообщения о реализованных в системе мерах защиты информации вход в систему означает согласие с необходимостью соблюдения правил и ограничений на работу с информацией.

Вход в систему в административном режиме

В тех случаях, когда необходимо получить доступ к компьютеру в обход действующих механизмов или прервать выполнение инициализации подсистем, администратор может использовать специальный административный режим входа.

Применение административного режима входа может потребоваться, в частности, в следующих ситуациях:

- при включенном режиме входа в систему "Только по идентификатору", если администратор не имеет персонального идентификатора;
- при повторяющихся ошибках функционального контроля, приводящих к длительному ожиданию инициализации защитных подсистем.

Внимание! Административный режим входа следует использовать только в крайних случаях для восстановления нормального функционирования системы. Выполнив вход в административном режиме, устраните возникшую проблему и перезагрузите компьютер.

Для входа в систему в административном режиме:

1. Перезагрузите компьютер.
2. Во время загрузки компьютера при появлении сообщений об инициализации системных сервисов Secret Net Studio нажмите комбинацию клавиш <Ctrl>+<Shift>+<Esc>.
3. При появлении экрана приветствия (приглашение на вход в систему) введите учетные данные администратора.

Смена пароля пользователя администратором

Смена пароля пользователя может быть выполнена самим пользователем или администратором. Описание смены пароля пользователем см. в документе [**3**].

Внимание!

- Для клиентов в сетевом режиме функционирования при включенном режиме усиленной аутентификации по паролю (см. стр.**14**) процедура административной смены пароля пользователя должна выполняться только в программе управления пользователями. При этом для выполнения процедуры администратору безопасности могут потребоваться дополнительные полномочия, предоставляемые при делегировании (см. раздел "Делегирование административных полномочий" в документе [**1**]). Если администратор сменит пароль пользователя с использованием других средств, новый пароль не будет сохранен в БД системы Secret Net Studio, что приведет к невозможности входа пользователя по этому паролю.
- Если пользователю присвоен персональный идентификатор и для этого идентификатора включены режимы хранения пароля и использования для входа в ПАК "Соболь", то в этом случае пароль не должен содержать символы кириллицы. Иначе после обработки идентификатора будет утеряна возможность его использования для входа в ПАК "Соболь".

Для смены пароля пользователя администратором:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В списке пользователей вызовите контекстное меню нужного пользователя и выберите команду "Смена пароля".

   На экране появится диалог для ввода пароля.
3. Введите новый пароль пользователя, установите отметку в поле "Синхронизировать данные пользователя на сервере аутентификации" и нажмите кнопку "ОК".

   Если пароль пользователя хранится в персональных идентификаторах, на экране появится диалог со списком персональных идентификаторов данного пользователя.
4. Предъявите все указанные в списке идентификаторы (см. стр.**30**).

Новый пароль будет записан в идентификаторы и их статус изменится на "Обработан", а кнопка "Отмена" изменит название на "Закрыть".

Примечание. Если при предъявлении идентификаторов будут допущены нарушения, сообщение об ошибке появится в таблице диалога в столбце "Статус".

5. Нажмите кнопку "Закрыть".

Использование ПАК "Соболь" в режиме интеграции с Secret Net Studio

В Secret Net Studio предусмотрен режим интеграции с ПАК "Соболь", обеспечивающий реализацию следующих возможностей:

- вход доменных или локальных пользователей в систему на компьютерах с ПАК "Соболь" с помощью персонального идентификатора, инициализированного и присвоенного пользователю средствами Secret Net Studio;
- формирование заданий на контроль целостности для ПАК "Соболь" средствами управления Secret Net Studio (см. стр.**112**);
- передача значений параметров "Минимальная длина пароля" и "Количество неудачных попыток аутентификации" в ПАК "Соболь" в соответствии с таблицей ниже;

Параметр в Secret Net Studio	**Параметр в ПАК "Соболь"**
Минимальная длина пароля	Минимальная длина пароля
Количество неудачных попыток аутентификации	Предельное число неудачных входов пользователя

- автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net Studio (см. таблицу ниже).

События комплекса "Соболь"	**События системы Secret Net Studio**
Вход пользователя	Соболь: вход пользователя
Вход администратора	
Не рассчитаны контрольные суммы	Соболь: не рассчитаны контрольные суммы
Переход в автономный режим	Соболь: изменение режима работы или Соболь: изменение режима использования
В версиях 3.x — Переход в сетевой режим В версии 4 — Переход в режим совместного использования	
В версиях 3.x — Удаление системного журнала В версии 4 — Удаление журнала	Соболь: очистка журнала
В версиях 3.x — Ошибка КС внешнего запроса В версии 4 — Ошибка внешнего запроса	Соболь: ошибка синхронизации параметров
Перерасчет контрольных сумм	Соболь: перерасчет контрольных сумм
Автоматический перерасчет КС	
Смена аутентификатора администратора	Соболь: смена аутентификатора
Смена аутентификатора пользователя	
Идентификатор не зарегистрирован	Соболь: запрет входа пользователя
Неправильный пароль	
Превышено число попыток входа	
Пользователь блокирован	

События комплекса "Соболь"	**События системы Secret Net Studio**
Ошибка при контроле целостности	Соболь: нарушена целостность ресурса
Обработаны внешние запросы	Соболь: синхронизация параметров
Добавлен новый пользователь	
Пользователь удален	
Добавление пользователя	
Удаление пользователя	
Администратор сменил свой пароль	Соболь: смена пароля
Администратор сменил пароль пользователя	
Пользователь сменил свой пароль	
Ошибка КС в памяти идентификатора	Соболь: ошибка КС в памяти идентификатора
Изменены параметры загрузочного диска	Соболь: изменены параметры загрузочного диска
Изменение шаблонов КЦ	
Изменены учетные номера	
Импорт ресурсов	
Обновление ключа КЦ	
Ошибка обновления ключа КЦ	
Попытка входа пользователя в запрещенное время	
Сработал механизм сторожевого таймера	
Экспорт ресурсов	
В версии 4 — Время/дата установки пароля опережает системное	Соболь: изменено системное время и дата
В версии 4 — Изменено системное время и дата	
В версии 4 — Обнаружен перевод системной даты назад	
В версии 4 — Скорректировано время последнего входа	
В версии 4 — Ошибка при экспорте журнала	Соболь: ошибка при экспорте журнала событий
В версии 4 — Экспорт журнала завершен	Соболь: экспорт журнала событий

Следует обратить внимание на следующие особенности включения режима интеграции для компьютеров с установленным клиентом в сетевом режиме функционирования:

1. При инициализации всех ПАК "Соболь" необходимо использовать один общий идентификатор администратора ПАК "Соболь" или его копии.

   Внимание! При инициализации ПАК "Соболь" версии 4.3 и выше должна быть выбрана версия математических преобразований "1989" (см. документацию ПАК "Соболь").

2. После установки ПАК "Соболь" на АРМ администратора безопасности и перевода его в режим совместного использования администратор безопасности должен сгенерировать ключи централизованного управления и записать их в идентификатор.

3. После подключения ПАК "Соболь" к системе Secret Net Studio администратор безопасности должен включить для своего персонального идентификатора режим разрешения входа в ПАК "Соболь". Включение режима осуществляется при настройке режимов использования идентификатора (см. стр.**34**).

Интеграция комплексов "Соболь" и Secret Net Studio

Включение и настройка режима интеграции комплексов "Соболь" и системы Secret Net Studio осуществляется в следующем порядке:

1. Для клиентов в сетевом режиме функционирования — на рабочем месте администратора безопасности выполните действия:
   - установите ПАК "Соболь". При установке выполните первичную регистрацию администратора и создайте необходимое количество резервных копий идентификатора администратора. После установки переведите комплекс из автономного режима в режим совместного использования. Сведения об установке и настройке ПАК "Соболь" см. в документации на изделие;
   - установите клиентское ПО системы Secret Net Studio в сетевом режиме функционирования (см. документ [**1**]);
   - сгенерируйте ключи централизованного управления комплексами "Соболь" (см. ниже);
   - подключите ПАК "Соболь" к Secret Net Studio (см. ниже);
   - при интеграции с ПАК "Соболь" версии 4 — предъявите идентификатор администратора комплекса;
   - настройте параметры пользователей для организации их доступа к компьютерам домена (назначение идентификаторов, паролей, формирование списка разрешенных компьютеров).
2. На каждом защищаемом компьютере выполните следующие действия:
   - установите ПАК "Соболь" с учетом следующих особенностей:
     - при установке для использования с клиентом в сетевом режиме функционирования выполните повторную регистрацию администратора с использованием идентификатора, подготовленного при выполнении действия **1**;
     - при интеграции с ПАК "Соболь" версий 3.x укажите ту же версию криптографической схемы, которая была задана на рабочем месте администратора безопасности. После установки переведите комплекс из автономного режима в режим совместного использования;

     Примечание. Сведения об установке и настройке ПАК "Соболь" см. в документации на изделие.
   - установите ПО системы Secret Net Studio в сетевом режиме функционирования (см. документ [**1**]);
   - подключите ПАК "Соболь" к Secret Net Studio (см. ниже);
   - при интеграции с ПАК "Соболь" версии 4 — предъявите идентификатор администратора комплекса.
3. На компьютерах с клиентом в автономном режиме функционирования выполните следующие действия:
   - установите ПАК "Соболь" в следующем порядке:
     - при установке выполните первичную или вторичную регистрацию администратора и создайте необходимое количество резервных копий идентификатора администратора;
     - после установки переведите комплекс из автономного режима в режим совместного использования;

     Примечание. Сведения об установке и настройке ПАК "Соболь" см. в документации на изделие.

- установите клиентское ПО системы Secret Net Studio в автономном режиме функционирования (см. документ [**1**]);
- подключите ПАК "Соболь" к Secret Net Studio (см. ниже);
- при интеграции с ПАК "Соболь" версии 4 — предъявите идентификатор администратора комплекса;
- настройте параметры пользователей и персональных идентификаторов.

Генерация ключей централизованного управления

Процедура генерации ключей централизованного управления ПАК "Соболь" выполняется в программе управления пользователями.

Для генерации ключей:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Генерация ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите идентификатор (см. стр.**30**), предназначенный для хранения ключей ЦУ комплексами "Соболь". По окончании процедуры генерации и записи ключей нажмите кнопку "ОК".

Предупреждение. Не допустите потери ключей ЦУ. В случае их утраты необходимо заново создать структуру централизованного управления комплексами "Соболь".

Подключение комплекса "Соболь" к Secret Net Studio

Для подключения комплекса:

1. В Панели управления Windows выберите ярлык "Управление Secret Net Studio".

   На экране появится диалоговое окно "Управление Secret Net Studio".
2. Перейдите к диалогу "Управление ПАК "Соболь".
3. Выполните следующие действия:
   - при необходимости введите заводской номер изделия в соответствующем поле и нажмите кнопку "Применить". Заводской номер указан в паспорте изделия, а также на самой плате;

     Примечание. Заводской номер заполняется также в комплексе "Соболь", но приоритетным является значение в Secret Net Studio.
   - для подключения комплекса "Соболь" нажмите кнопку "Подключить".

     Примечание. После подключения комплекса "Соболь" в диалоге "Управление ПАК "Соболь" появится поле "Разрешить автоматическую загрузку ОС". Установите в нем отметку, если необходимо организовать автоматический вход в ПАК "Соболь" без предъявления персонального идентификатора. Режим автоматического входа в комплекс "Соболь" начнет действовать после перезагрузки операционной системы компьютера.
4. На компьютере с установленным клиентом в сетевом режиме функционирования на экране появится диалог с предложением предъявить ключевой носитель (идентификатор) с ключами ЦУ комплексами "Соболь". В этом случае предъявите нужный идентификатор.

   Система Secret Net Studio перейдет в режим интеграции с комплексом "Соболь" и на экране появится сообщение об этом.
5. Нажмите кнопку "ОК" в диалоговом окне "Управление Secret Net Studio".

Отключение режима интеграции Secret Net Studio и "Соболь"

Для отключения режима интеграции:

1. В Панели управления Windows выберите ярлык "Управление Secret Net Studio".

   На экране появится диалоговое окно "Управление Secret Net Studio".
2. Перейдите к диалогу "Управление ПАК "Соболь".

3. Нажмите кнопку "Отключить".

   Режим интеграции с комплексом "Соболь" будет отключен и на экране появится сообщение об этом.

   Внимание! Повторное включение в Secret Net Studio режима интеграции с комплексом "Соболь" возможно только после перезагрузки компьютера.

4. Если не планируется дальнейшее использование режима интеграции, при следующей загрузке компьютера войдите с правами администратора в комплекс "Соболь" и переведите изделие в автономный режим работы (см. документацию на изделие).

Управление ключами централизованного управления ПАК "Соболь"

Операции с ключами централизованного управления ПАК "Соболь" выполняются в программе управления пользователями.

Загрузка ключей

Для выполнения операций с использованием ключей централизованного управления ПАК "Соболь" (предоставление пользователям доступа к компьютерам, работа с ключами администратора ПАК) их необходимо загрузить. Ключи сохраняются в системе до закрытия программы управления пользователями.

Для загрузки ключей:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Загрузка ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите носитель (см. стр. **30**), на котором хранятся ключи централизованного управления ПАК "Соболь".

   После успешной загрузки ключей на экране появится сообщение об этом.

Копирование ключей

В целях повышения надежности хранения ключей рекомендуется сохранять их копии на нескольких идентификаторах.

Для копирования ключей:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Копирование ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите идентификатор (см. стр.**30**), содержащий копируемые ключи централизованного управления ПАК "Соболь".

   Выполнится считывание ключей, после чего на экране появится следующий диалог для предъявления идентификатора.
4. Предъявите идентификатор, на который требуется записать ключи.

   При успешной записи ключей в идентификатор его статус изменится на "Обработан".
5. Нажмите кнопку "Закрыть".

Удаление ключей

Предупреждение. Удаление ключей централизованного управления ПАК "Соболь" осуществляется без возможности их восстановления в том же виде. Процедура приводит к необратимым последствиям очистки всех параметров текущей схемы централизованного управления ПАК "Соболь" в домене. Если возникнет необходимость вернуться к такой схеме, потребуется полная переинициализация централизованного управления ПАК "Соболь" во всем домене. Переинициализация выполняется в следующей последовательности:

- генерация новых ключей централизованного управления ПАК "Соболь";

- включение для электронных идентификаторов режима интеграции с ПАК "Соболь";
- настройка доступа пользователей к компьютерам;
- выполнение на каждом компьютере с ПАК "Соболь" процедур отключения режима интеграции с Secret Net Studio и подключения комплекса "Соболь" к системе.

Для удаления ключей:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Удаление ключей ЦУ ПАК "Соболь".

   На экране появится сообщение о последствиях выполнения процедуры.
3. Нажмите кнопку "Да" в окне сообщения.

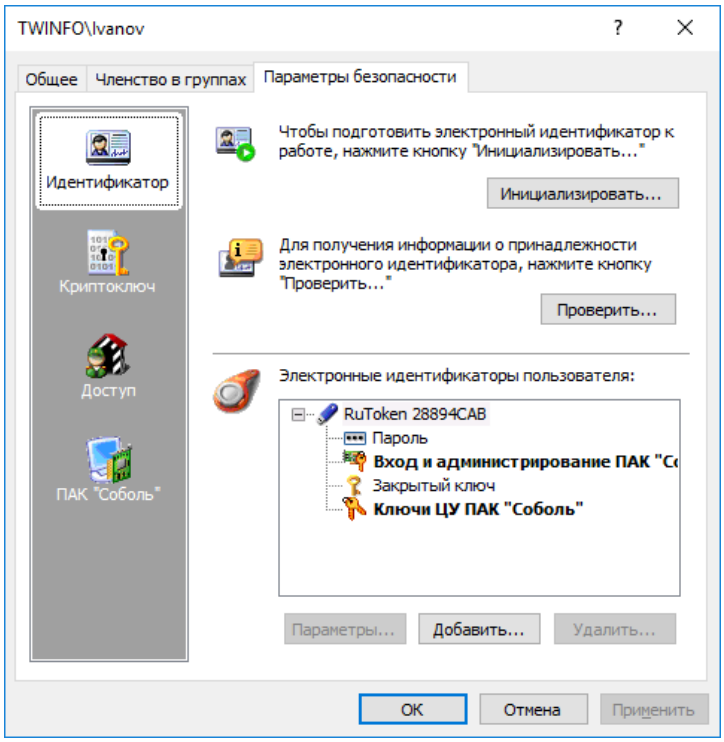
   На экране появится запрос на продолжение операции.
4. Нажмите кнопку "Да" в диалоге запроса.

   Произойдет удаление ключей из системы, после чего на экране появится запрос на удаление ключей из идентификаторов.
5. Предъявите идентификатор, на котором хранятся ключи.

   Ключи будут удалены из идентификатора.

Копирование идентификатора администратора ПАК "Соболь"

В Secret Net Studio идентификатор администратора ПАК "Соболь" может быть присвоен пользователю системы. После присвоения такой идентификатор отображается в списке идентификаторов пользователя со специальным признаком:



Если при инициализации ПАК "Соболь" не было создано достаточное количество резервных копий идентификаторов, можно скопировать содержимое идентификатора администратора ПАК "Соболь" на другой носитель. Новый идентификатор также можно будет использовать для администрирования комплексов "Соболь".

Чтобы копировать идентификатор администратора ПАК "Соболь" для доменного пользователя (для клиентов в сетевом режиме функционирования), предварительно загрузите ключи централизованного управления ПАК "Соболь" (см. стр.**24**).

Для копирования идентификатора администратора ПАК "Соболь":

1. Запустите программу управления пользователями (см. стр.**270**).

2. В меню "Сервис" выберите команду "Копирование идентификатора администратора ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".

3. Предъявите идентификатор (см. стр.**30**) администратора ПАК "Соболь".

   На экране появится диалог запроса пароля.

4. Введите пароль администратора ПАК "Соболь" и нажмите кнопку "ОК".

   На экране появится следующий диалог для предъявления идентификатора.

5. Предъявите идентификатор, в который должны быть скопированы сведения из идентификатора администратора ПАК "Соболь".

   После успешной записи сведений в идентификатор его статус примет значение "Обработан".

6. Нажмите кнопку "ОК".

Предоставление доступа к компьютерам с ПАК "Соболь"

На определенных компьютерах с клиентом в сетевом режиме функционирования и ПАК "Соболь" в режиме интеграции с Secret Net Studio пользователям можно предоставить возможность входа в ПАК "Соболь" и далее в систему с использованием персональных идентификаторов, инициализированных и присвоенных средствами системы защиты. То есть для входа в ПАК "Соболь" и для входа в систему пользователь может использовать один идентификатор.

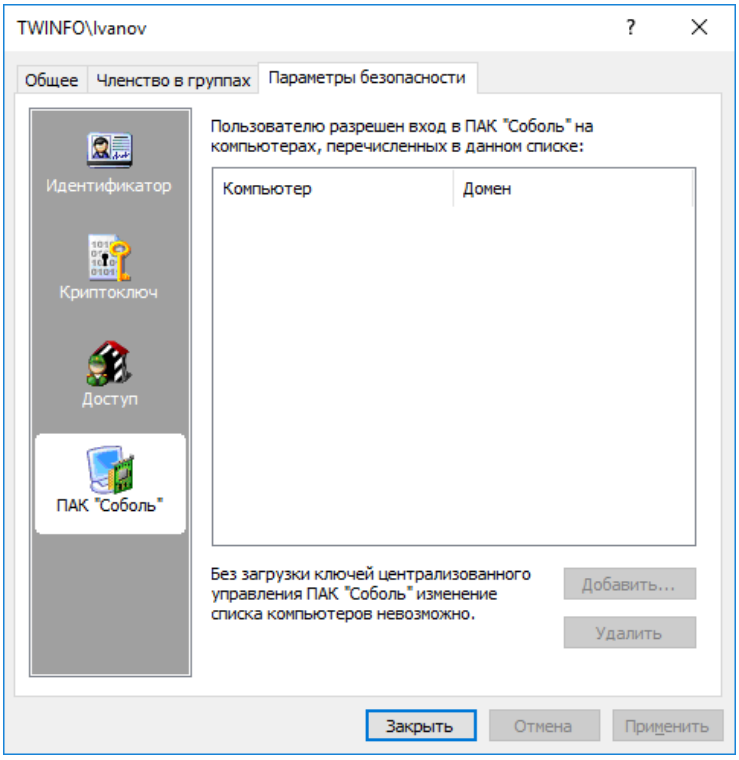
Чтобы предоставить такую возможность доменному пользователю, необходимо выполнить следующие действия:

- присвоить пользователю идентификатор с включенным режимом разрешения входа в ПАК "Соболь" (см. стр.**31**). Для идентификаторов, присвоенных пользователю ранее, включить режим можно при настройке режимов использования идентификатора (см. стр.**34**);
- сформировать список компьютеров, на которых пользователю разрешается выполнять вход в ПАК "Соболь" (см. процедуру ниже).

Перед формированием списка компьютеров предварительно загрузите ключи централизованного управления ПАК "Соболь" (см. стр.**24**).

Для формирования списка компьютеров:

1. В программе управления пользователями вызовите окно настройки свойств доменного пользователя и перейдите к диалогу "Параметры безопасности" (см. стр.**270**).
2. В панели выбора групп параметров выберите группу "ПАК "Соболь".



3. Нажмите кнопку "Добавить".

   На экране появится стандартный диалог ОС Windows для выбора объектов.
4. Выберите компьютеры, к которым пользователь должен иметь доступ, и добавьте их в список.
5. Если требуется удалить компьютер из списка, выберите его и нажмите кнопку "Удалить".
6. Завершив формирование списка компьютеров, нажмите кнопку "Закрыть" или "Применить" в окне настройки свойств пользователя.

Особенности аутентификации при использовании учетной записи Microsoft

Механизм защиты входа в систему по-разному взаимодействует с учетными записями Microsoft в зависимости от используемой версии ОС Windows.

Windows 8 – Windows 10

В данных системах пользователи с учетной записью Microsoft могут выполнять вход по электронному идентификатору только на компьютерах, входящих в домен.

В Windows 10 версии 2004 дополнительно действует ограничение, не позволяющее выбрать уровень конфиденциальности сессии при включенном контроле потоков. Для снятия данного ограничения требуется отключить параметр "Требовать выполнение входа с помощью Windows Hello для учетных записей Майкрософт" в настройках учетных записей Windows.

Подробные сведения о настройке механизма полномочного управления доступом содержатся на стр.158.

Глава 2
Работа с персональными идентификаторами

Управление персональными идентификаторами

Персональный идентификатор — устройство для хранения информации, необходимой при идентификации и аутентификации пользователя. В идентификаторе могут храниться ключи для работы с зашифрованными данными в криптоконтейнерах.

В Secret Net Studio могут использоваться персональные идентификаторы eToken, Rutoken, JaCarta, ESMART, Guardant ID, vdToken или идентификаторы iButton.

Полный список идентификаторов приведен в таблице ниже.

Продукт	USB-ключи	Смарт-карты
eToken PRO (Java)	eToken PRO (Java)	eToken PRO (Java) SC
JaCarta PKI	JaCarta PKI JaCarta PKI Flash	JaCarta PKI SC
JaCarta PKI/BIO	JaCarta PKI/BIO Jacarta-2 PKI/BIO/ГОСТ	JaCarta PKI/BIO JaCarta PKI/BIO/ГОСТ Jacarta-2 PKI/BIO/ГОСТ
JaCarta ГОСТ	JaCarta ГОСТ JaCarta PKI/ГОСТ JaCarta ГОСТ Flash	JaCarta ГОСТ SC
JaCarta-2 ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ	JaCarta-2 PKI/ГОСТ SC
JaCarta SF/ГОСТ	JaCarta SF/ГОСТ	—
JaCarta PRO	JaCarta PRO JaCarta-2 PRO/ГОСТ	JaCarta PRO SC JaCarta-2 PRO/ГОСТ SC
JaCarta WebPass	JaCarta WebPass	—
JaCarta-2 SE	JaCarta-2 SE	—
JaCarta U2F	JaCarta U2F	—
JaCarta LT	JaCarta LT	—
RuToken S	RuToken S (версия 2.0) RuToken S (версия 3.0)	—
RuToken ЭЦП	RuToken ЭЦП RuToken ЭЦП 2.0 RuToken ЭЦП Touch RuToken ЭЦП PKI RuToken ЭЦП 2.0 Flash RuToken ЭЦП Bluetooth RuToken ЭЦП 2.0 Touch RuToken ЭЦП 2.0 Flash Touch	RuToken ЭЦП SC RuToken ЭЦП 2.0 SC
RuToken Lite	RuToken Lite	RuToken Lite SC
RuToken 2151	RuToken 2151	RuToken 2151 SC
ESMART Token	ESMART Token	ESMART Token SC
ESMART Token ГОСТ	ESMART Token ГОСТ ESMART Token ГОСТ D	ESMART Token ГОСТ SC ESMART Token ГОСТ D SC

Продукт	USB-ключи	Смарт-карты
Guardant ID	Guardant ID Guardant ID 2.0	—
vdToken	vdToken 2.0	—
R301 Foros	R301 Foros	R301 Foros

Пояснение. Для хранения ключей шифрования данных могут также использоваться сменные носители, такие как флеш-карты или USB-флеш-накопители. Далее термин "идентификатор" будет применяться и к сменным носителям, которые выступают в качестве ключевых носителей и присваиваются пользователям.

Персональный идентификатор выдается пользователю администратором. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно. При этом одному пользователю можно присвоить несколько идентификаторов. Если используется ПАК "Соболь" в режиме интеграции с Secret Net Studio, максимально возможное количество присвоенных идентификаторов для одного пользователя — 32.

Администратор безопасности может выполнять следующие операции с персональными идентификаторами:

Инициализация идентификатора
Форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net Studio. Инициализация требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных. Форматированию подлежат также и сменные носители, предназначенные для хранения ключей
Присвоение идентификатора
Добавление в базу данных Secret Net Studio сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером
Отмена присвоения идентификатора
Удаление из базы данных Secret Net Studio информации о принадлежности данного персонального идентификатора данному пользователю. Далее для простоты эту операцию будем называть "удаление идентификатора"
Включение режима хранения пароля в идентификаторе
Добавление в базу данных Secret Net Studio сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией может выполняться запись пароля в идентификатор. После включения режима и записи пароля в идентификатор пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора
Отключение режима хранения пароля в идентификаторе
Операция, противоположная предыдущей. Одновременно с отключением режима хранения выполняется удаление пароля из памяти персонального идентификатора. Идентификатор остается закрепленным за пользователем
Включение и отключение режима разрешения входа в ПАК "Соболь"
При включенном режиме пользователю разрешено использовать для входа в ПАК "Соболь" идентификатор, присвоенный в системе Secret Net Studio
Запись и удаление ключей для работы с зашифрованными данными
Используется для хранения в идентификаторе (или на сменном носителе) ключей для работы с зашифрованными данными в криптоконтейнерах
Проверка принадлежности
С помощью этой операции администратор безопасности может проверить, кому из пользователей присвоен данный персональный идентификатор

Основные операции с идентификаторами

Предъявление идентификатора

Предъявление идентификатора выполняется по требованию системы для записи или считывания информации.

Для предъявления USB-ключа или смарт-карты:

- Если точно известно, какой идентификатор нужно предъявить, вставьте его в разъем USB-порта компьютера или приложите к считывающему устройству.
- Если нужно выбрать идентификатор из нескольких имеющихся, удалите отметку из поля "Использовать первый предъявленный идентификатор" и поочередно предъявляйте идентификаторы. При этом серийный номер каждого предъявляемого идентификатора будет отображаться в диалоге. Когда нужный идентификатор найден, нажмите кнопку "ОК".

Примечание. Если предъявлен идентификатор, который защищен **нестандартным** PIN-кодом (паролем), на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

Для предъявления идентификатора iButton:

- Если точно известно, какой идентификатор нужно предъявить, прислоните его к считывателю и удерживайте в таком положении до закрытия диалога "Предъявите идентификатор".
- Если нужно выбрать идентификатор из нескольких имеющихся, удалите отметку из поля "Использовать первый предъявленный идентификатор" и поочередно предъявляйте идентификаторы. При этом серийный номер каждого предъявляемого идентификатора будет отображаться в диалоге. Когда нужный идентификатор найден, не прерывая контакт этого идентификатора со считывающим устройством, нажмите кнопку "ОК".

Для предъявления другого сменного носителя:

1. Вставьте сменный носитель в разъем компьютера и нажмите кнопку "Диск".

   В диалоге появится наименование сменного носителя.
2. Выберите в списке это наименование и нажмите кнопку "ОК".

Сообщения об ошибках

Если при предъявлении идентификатора произошли ошибки, на экране появится сообщение, поясняющее причину ошибки. В таблице перечислены возможные причины ошибок и действия, которые необходимо предпринять для их устранения.

Причина	Действие
Нарушение контакта идентификатора со считывателем или недостаточная его продолжительность	Предъявите идентификатор повторно с учетом общих требований по использованию идентификаторов
Предъявленный идентификатор принадлежит другому пользователю	Процедура будет прервана. Предъявите идентификатор, принадлежащий данному пользователю, или идентификатор, который никому не принадлежит
Был предъявлен идентификатор, уже содержащий сведения системы Secret Net Studio или ПАК "Соболь"	Если удаление сведений, содержащихся в идентификаторе, допустимо, можно продолжить выполняемую процедуру
Нарушена структура данных в идентификаторе	Выполните инициализацию идентификатора и повторите действие

Инициализация идентификатора

Для инициализации идентификатора:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Инициализация идентификатора".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите идентификатор (см. выше).

   Произойдет инициализация идентификатора, после чего на экране появится соответствующее сообщение.

Проверка принадлежности

Для проверки принадлежности идентификатора:

1. Запустите программу управления пользователями (см. стр.**270**).
2. В меню "Сервис" выберите команду "Проверка идентификатора".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите проверяемый идентификатор (см. стр.**30**).

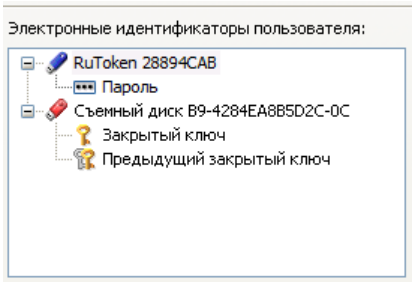
   Если в базе данных Secret Net Studio есть сведения об этом идентификаторе, они будут выведены на экран.

Работа с идентификаторами пользователей

Просмотр сведений об идентификаторах пользователя

Сведения о персональных идентификаторах пользователя представлены в программе управления пользователями (см. стр. **270**). Для просмотра сведений откройте диалоговое окно настройки свойств пользователя, перейдите к диалогу "Параметры безопасности" и выберите группу параметров "Идентификатор".

Сведения представлены в виде списка присвоенных идентификаторов:



Для каждого идентификатора указаны тип и серийный номер. Дополнительно могут быть указаны следующие признаки хранения служебной информации:

- признак хранения пароля;
- признаки хранения в идентификаторе ключей для работы с зашифрованными данными в криптоконтейнерах;
- признак использования идентификатора для входа в ПАК "Соболь";
- признак использования идентификатора для входа и администрирования ПАК "Соболь";
- признак хранения ключей централизованного управления ПАК "Соболь".

Присвоение идентификатора

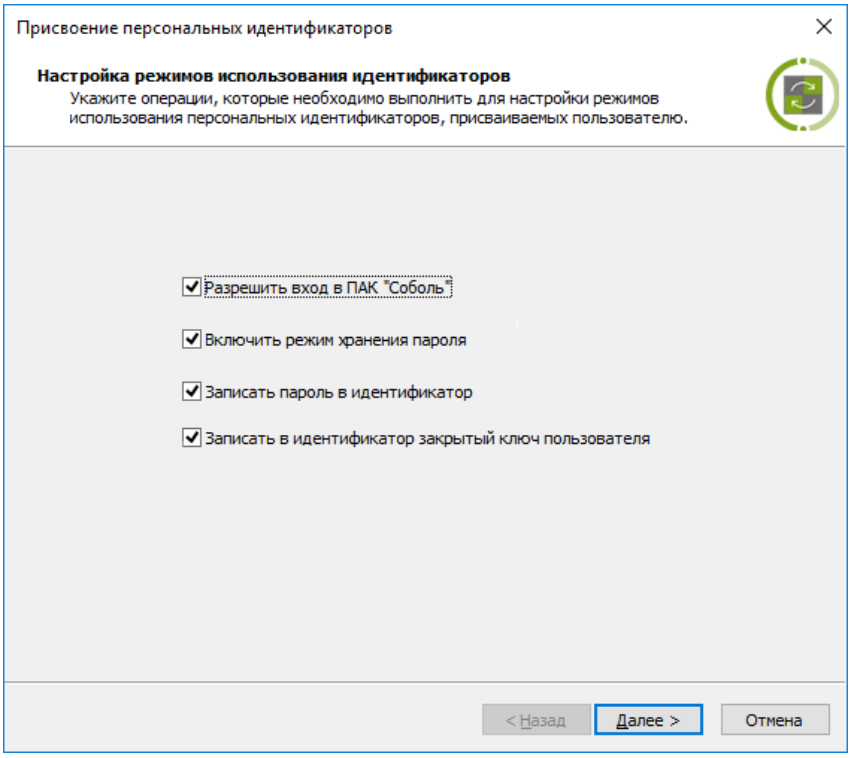
Процедура присвоения идентификатора пользователю выполняется с помощью программы-мастера. При присвоении можно настроить режимы использования персонального идентификатора.

Примечания:
- Для записи пароля в идентификатор потребуется ввести пароль данного пользователя.
- Для записи в идентификатор уже имеющегося у пользователя ключа для шифрования данных (закрытого ключа) потребуется предъявить идентификатор, на котором этот ключ записан.
- Если идентификатор принадлежит администратору ПАК "Соболь", то пароль пользователя Windows и пароль входа в ПАК "Соболь" должны совпадать.
- Для включения режима разрешения входа с помощью идентификатора в ПАК "Соболь" необходимо, чтобы ПАК функционировал в режиме интеграции с Secret Net Studio (см. стр.20).

Для присвоения идентификатора пользователю:

1. Запустите программу управления пользователями (см. стр.270).
2. Вызовите окно настройки свойств пользователя, перейдите к диалогу "Параметры безопасности" и нажмите кнопку "Добавить".

   На экране появится стартовый диалог мастера присвоения идентификаторов.



3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".

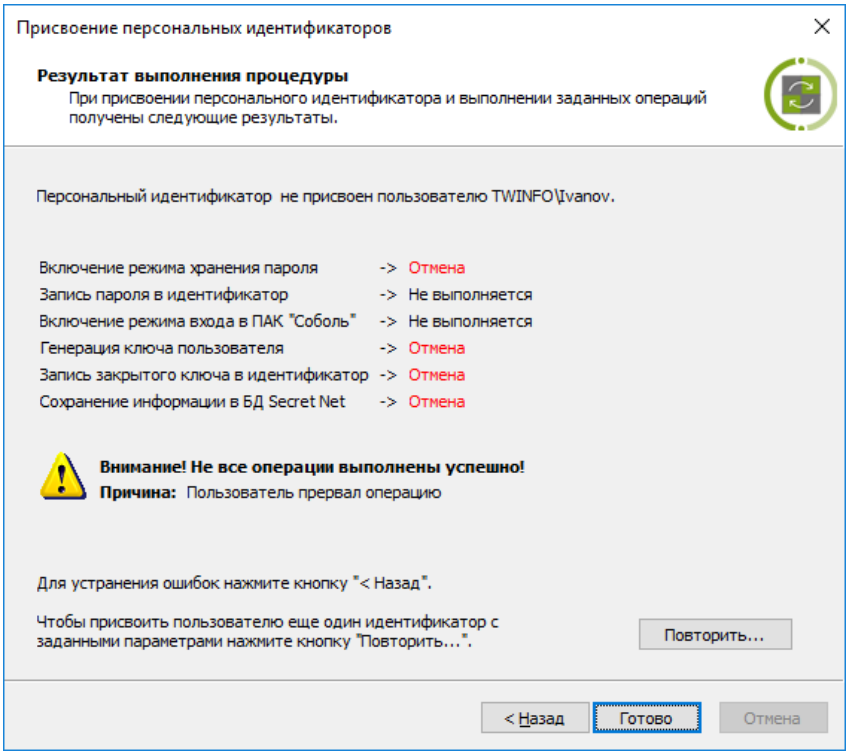
   На экране появится диалог, отображающий ход выполнения операций.
4. Если выбрана операция "Записать пароль в идентификатор", "Разрешить вход в ПАК "Соболь" или "Записать в идентификатор закрытый ключ пользователя", выполните действия по запросу программы:
   - При появлении диалога "Ввод пароля" введите пароль пользователя.
   - При появлении диалога "Предъявите идентификатор" предъявите идентификатор пользователя (см. стр.30), содержащий его закрытый ключ.

   Успешно выполненные операции имеют статус "Выполнено". Если при выполнении операции произошла ошибка, в диалоге будет приведено соответствующее сообщение об этом.
5. После успешного выполнения всех операций нажмите кнопку "Далее >".

   На экране появится диалог "Предъявите идентификатор".
6. Предъявите идентификатор (см. стр.30) для присвоения пользователю и записи данных. Не нарушайте контакт идентификатора со считывателем до завершения всех операций.

Ошибки записи данных

В процессе записи данных могут произойти ошибки (например, связанные с идентификатором или БД), которые отображаются в диалоге с результатами выполнения:



Внимание! Идентификатор не будет присвоен, если произошла ошибка при выполнении какой-либо операции или эта операция отменена из-за других ошибок. Для устранения ошибок нажмите кнопку "< Назад" и повторно предъявите идентификатор.

После успешного завершения всех предусмотренных операций статус каждой из них должен иметь значение "Выполнено".

7. Чтобы присвоить пользователю еще один идентификатор с такими же параметрами, нажмите кнопку "Повторить...".
8. Для завершения работы нажмите кнопку "Готово".

Присвоение идентификатора другого пользователя

В процессе присвоения идентификатора выполняется проверка его принадлежности другому пользователю и наличия в идентификаторе ранее сохраненных структур Secret Net Studio или ПАК "Соболь". Если идентификатор уже присвоен другому пользователю, о котором имеются сведения в данной системе, операция присвоения прерывается с выдачей соответствующего сообщения.

Если предъявленный идентификатор содержит данные Secret Net Studio или ПАК "Соболь", но не принадлежит никому из пользователей данной системы (например, используется для входа локального пользователя на другом компьютере), выводится запрос на продолжение действий. В этом случае возможны следующие варианты:

- Идентификатор содержит закрытый ключ (или пару ключей — текущий и предыдущий), но пользователь, которому присваивается идентификатор, уже имеет свой ключ — в этом варианте система предлагает заменить ключи в идентификаторе. При продолжении процедуры закрытый ключ из идентификатора будет удален. Запись текущего закрытого ключа пользователя в идентификатор осуществляется, если в мастере присвоения выбрана операция "Записать в идентификатор закрытый ключ пользователя" (см. выше).

- Идентификатор содержит закрытый ключ (или пару ключей — текущий и предыдущий), и пользователь, которому присваивается идентификатор, не имеет своего ключа — в этом варианте выводится запрос на использование ключей из идентификатора для пользователя. Чтобы оставить ключ в идентификаторе и использовать его для пользователя, которому этот идентификатор присваивается, нажмите кнопку "Да" в диалоге запроса. При нажатии кнопки "Нет" закрытый ключ из идентификатора будет удален. Генерация и запись нового закрытого ключа пользователя в идентификатор осуществляются, если в мастере присвоения выбрана операция "Записать в идентификатор закрытый ключ пользователя" (см. выше). Для отмены процедуры присвоения идентификатора нажмите кнопку "Отмена".

  Примечание. За счет использования ключа из идентификатора (ответ "Да" в диалоге запроса) можно реализовать, например, работу с одним криптоконтейнером с помощью этого идентификатора для различных локальных пользователей на нескольких компьютерах. В автономном режиме функционирования клиента идентификатор можно будет использовать как для локальных, так и для доменных пользователей компьютера.

- Идентификатор содержит другие данные Secret Net Studio или ПАК "Соболь" — выводится запрос для подтверждения операций удаления обнаруженных данных. Если вы уверены, что этим идентификатором никто больше не пользуется, нажмите кнопку "Да" и повторно предъявите данный идентификатор.

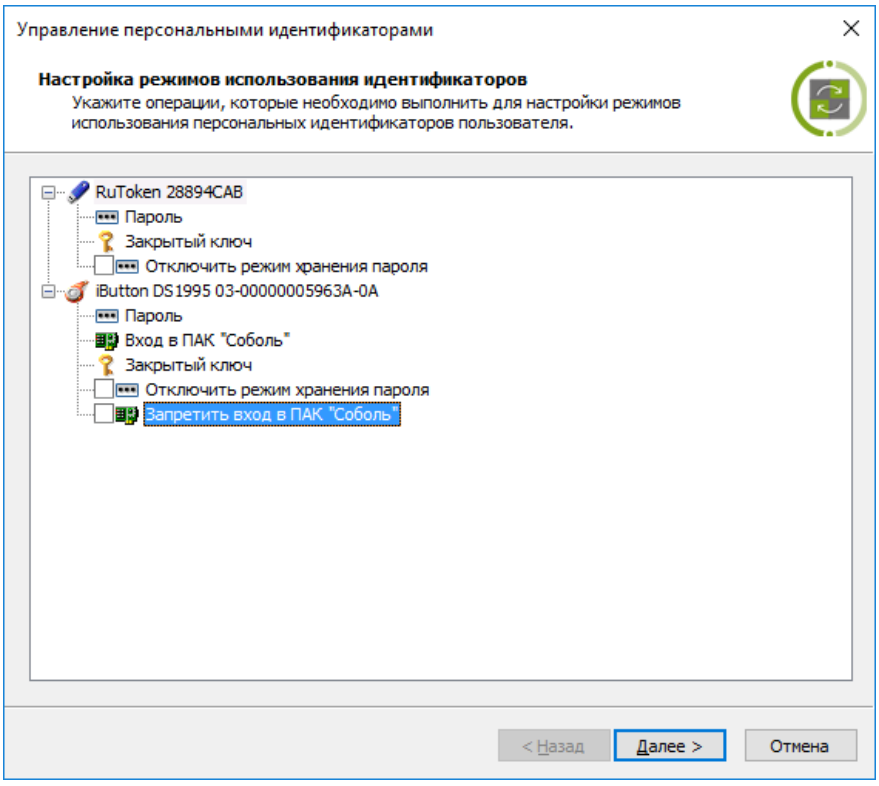
Настройка режимов использования идентификаторов

При необходимости можно изменить действующие режимы использования идентификаторов (кроме сменных носителей), присвоенных пользователю. Процедура настройки режимов выполняется с помощью программы-мастера.

Для настройки режимов идентификаторов пользователя:

1. Запустите программу управления пользователями (см. стр.**270**).
2. Вызовите окно настройки свойств пользователя, перейдите к диалогу "Параметры безопасности" и нажмите кнопку "Параметры".

   На экране появится стартовый диалог мастера настройки режимов.



   Диалог содержит список идентификаторов, присвоенных пользователю.

Примечание. Сменные диски, присвоенные пользователю, в списке не отображаются.

Для каждого идентификатора в списке указаны включенные режимы и доступные для выполнения операции. Например, если для идентификатора включен режим хранения пароля, то доступной операцией будет "Отключить режим хранения пароля".

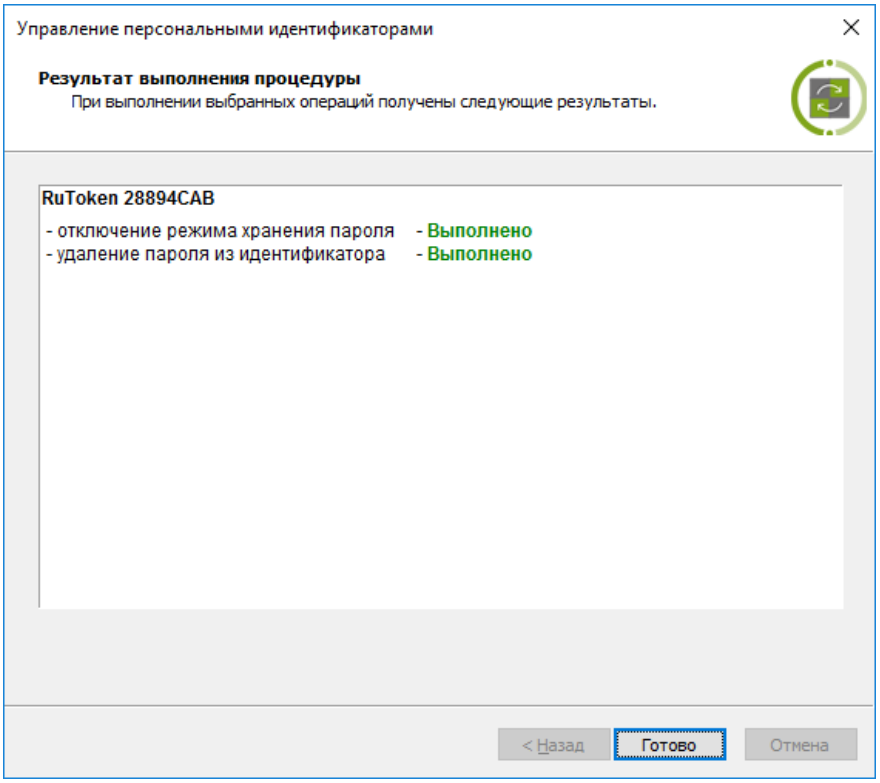
3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".
4. Если выбрана операция "Записать пароль в идентификатор" или "Разрешить вход в ПАК "Соболь", на экране появится диалог "Ввод пароля". Введите пароль пользователя и нажмите кнопку "ОК".

   После успешного ввода пароля в диалоге справа от названия операции появится запись "Выполнено".
5. Нажмите кнопку "Далее >".

   Если была выбрана любая операция, кроме операции "Включить режим хранения пароля", на экране появится диалог "Предъявите идентификатор". В диалоге отображаются наименования идентификаторов, для которых были выбраны операции, и статус их обработки: "Не обработан".
6. Предъявите все идентификаторы, указанные в списке (см. стр.**30**).

   После успешного предъявления идентификатора его статус изменится на "Обработан". Если предъявление идентификатора выполнено с ошибкой, в столбце статуса обработки появится сообщение об ошибке. После предъявления всех идентификаторов кнопка "Отмена" будет заменена кнопкой "Закрыть".
7. Нажмите кнопку "Закрыть".

   На экране появится диалог с результатами выполнения операций. Если операции выполнены с ошибками, в диалоге будет приведено их описание.



После успешного завершения всех предусмотренных операций статус каждой из них должен иметь значение "Выполнено".

8. Для завершения работы нажмите кнопку "Готово".

Удаление идентификатора

После выполнения процедуры удаления идентификатора пользователь теряет возможность использовать идентификатор для входа в систему и хранить в нем пароль и ключи.

Для удаления идентификатора пользователя:

1. Запустите программу управления пользователями (см. стр.**270**).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. Выберите в списке идентификатор и нажмите кнопку "Удалить".

   Если выбранный идентификатор является единственным идентификатором, в котором хранятся ключи для работы с зашифрованными данными в криптоконтейнерах, на экране появится запрос на продолжение операции.
4. Нажмите кнопку "Да".

   На экране появится запрос на очистку памяти идентификатора.
5. Нажмите кнопку "Да".

   На экране появится диалог "Предъявите идентификатор".
6. Предъявите идентификатор (см. стр.**30**).

   Статус предъявленного идентификатора изменится на "Обработан".

   Примечание. Если при предъявлении идентификатора будут допущены нарушения, сообщение об ошибке появится в таблице диалога в столбце "Статус".
7. Нажмите кнопку "Закрыть".

   Запись об удаленном идентификаторе исчезнет из списка идентификаторов.

Глава 3
Настройка механизма защиты терминальных подключений

Использование идентификаторов в терминальных сессиях

Присвоенные пользователям персональные идентификаторы могут использоваться для терминального входа в подключениях удаленного доступа. Для этого на компьютере, который является терминальным сервером, должен быть включен любой из следующих режимов идентификации (см. стр.**14**):

- "Смешанный" (включен по умолчанию);
- "Только по идентификатору".

При этом в средствах подключения к удаленному рабочему столу (Remote Desktop Connection) версии 6.0 и выше по умолчанию требуется предварительная аутентификация пользователя. Предварительная аутентификация осуществляется путем ввода учетных данных пользователя (имя и пароль) до подключения к терминальному серверу. Из-за этого проявляются следующие особенности установления соединения:

- Если на терминальном сервере включен режим идентификации "Смешанный" — после предварительной аутентификации на терминальном клиенте сразу осуществляется терминальный вход по указанным учетным данным пользователя. Терминальный сервер не ожидает предъявление идентификатора.
- Если на терминальном сервере включен режим идентификации "Только по идентификатору" — при удаленном подключении сначала выполняется предварительная аутентификация (пользователь вводит имя и пароль для инициирования подключения), а затем при соединении с терминальным сервером пользователю необходимо предъявить свой персональный идентификатор.

При отключенной предварительной аутентификации обеспечивается вход пользователя в терминальную сессию по идентификатору без предварительного запроса имени и пароля.

Отключение предварительной аутентификации

Требование предварительной аутентификации в средствах подключения к удаленному рабочему столу может действовать как на стороне терминального клиента, так и на стороне терминального сервера. Если запрос учетных данных пользователя отключен на стороне клиента, терминальный вход с этого компьютера будет возможен только на сервер с отключенным требованием предварительной аутентификации. При отключении требования на терминальном сервере удаленные подключения разрешаются для любых клиентов — и с включенной, и с отключенной предварительной аутентификацией.

Отключение на терминальном клиенте

Отключение предварительной аутентификации на стороне терминального клиента предусмотрено в средствах подключения к удаленному рабочему столу версии 6.0 и выше. Для получения сведений об используемой версии вызовите контекстное меню заголовка окна "Подключение к удаленному рабочему столу" (Remote Desktop Connection) и активируйте команду "О программе" (About).

Для отключения предварительной аутентификации на стороне терминального клиента:

1. Войдите в систему с учетными данными пользователя, который будет открывать терминальные сессии на этом компьютере.

2. В текстовом редакторе (например, Блокнот) загрузите файл Default.rdp из папки документов пользователя.

   Пояснения. Файл Default.rdp является скрытым системным файлом. Он автоматически создается в системной папке документов пользователя (%USERPROFILE%\Documents или %USERPROFILE%\My Documents) после первого терминального входа с этого компьютера и далее обновляется при изменении параметров подключения.
   Чтобы загрузить файл, в стандартном диалоге открытия файлов выберите системную папку документов (ярлык папки присутствует в левой части диалога) и в поле ввода имени файла введите Default.rdp.

3. Проверьте в тексте наличие строки с параметром enablecredsspsupport. Если параметр отсутствует, добавьте строку:

   enablecredsspsupport:i:0

   Примечание. При наличии указанного параметра проверьте заданное значение и при необходимости отредактируйте его.

4. Сохраните изменения.

Отключение на терминальном сервере

Для отключения предварительной аутентификации на стороне терминального сервера:

1. В Панели управления Windows перейдите к разделу "Система" (System) и в левой части окна выберите ссылку "Настройка удаленного доступа" (Remote settings).

   На экране появится диалоговое окно настройки свойств системы, в котором будет открыта вкладка с параметрами удаленного доступа.

2. Удалите отметку из поля, разрешающего подключения только с проверкой подлинности на уровне сети ("с сетевой проверкой подлинности", with Network Level Authentication). Для этого отметьте поле "Разрешить удаленные подключения к этому компьютеру" ("Разрешать подключения от компьютеров с любой версией удаленного рабочего стола", Allow connections from computers running any version of Remote Desktop).

   Примечание. Изменение поля, разрешающего подключения только с проверкой подлинности на уровне сети, может быть заблокировано действующей групповой политикой. В этом случае откройте соответствующую оснастку управления групповыми политиками и измените состояние параметра "Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети" (Require user authentication for remote connections by using Network Level Authentication). Параметр представлен в группе политик конфигурации компьютера, раздел "Административные шаблоны / Компоненты Windows / Службы удаленных рабочих столов / Узел сеансов удаленных рабочих столов / Безопасность" (Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Security).

3. Закройте диалоговое окно с сохранением сделанных изменений.

Программные методы обработки идентификаторов

В терминальных сессиях могут применяться различные методы обработки персональных идентификаторов, подключенных на терминальных клиентах. Предусмотрены следующие методы (перечислены в порядке приоритета использования):

1. Метод виртуальных каналов. Применяется в случае, если на терминальном клиенте установлено ПО клиента Secret Net Studio или СЗИ Secret Net начиная с версии 7.0. Метод не требует дополнительной настройки и доступен всегда (не отключается).

2. Метод на базе протокола RPC (Remote Procedure Call). Применяется в случае, если на терминальном клиенте установлено ПО клиента Secret Net Studio или СЗИ Secret Net начиная с версии 5.0. Для использования требуется дополнительная настройка TCP-портов для сетевых соединений (см. стр.**272**). Данный метод по умолчанию отключен. Для включения метода необходимо на компьютере терминального сервера в ключе системного реестра HKLM\Software\Infosec\Secret Net 5\HwSystem указать нулевое значение для параметра NoRemoteConnect.
3. Метод с использованием режима "Смарт-карты". Применяется в случае отсутствия установленного клиентского ПО на терминальном клиенте. Для использования метода необходимо включать режим "Смарт- карты" в параметрах удаленного подключения. Чтобы заблокировать возможность использования метода, в системном реестре терминального сервера в ключе HKLM\Software\Infosec\Secret Net 5\HwSystem создайте параметр NoSCRedirection типа REG_DWORD со значением 1.

Ограничение использования локальных устройств и ресурсов

Система Secret Net Studio предоставляет возможность заблокировать использование (перенаправление) локальных устройств и ресурсов компьютеров в терминальных подключениях по протоколу RDP. Блокировка осуществляется при включении запрета перенаправления определенных типов локальных устройств и ресурсов. Если в системе Secret Net Studio включен запрет перенаправления, пользователи не смогут использовать соответствующие локальные устройства и ресурсы своих компьютеров в терминальных сессиях (независимо от заданных параметров удаленного подключения).

Запрет перенаправления может действовать в зависимости от роли компьютера в удаленном подключении. Использование устройств и ресурсов можно блокировать на стороне терминального сервера (чтобы запрет действовал для всех "входящих" терминальных сессий), на стороне терминального клиента (для всех "исходящих" сессий) или независимо от роли компьютера в удаленном подключении.

Управление перенаправлением локальных устройств терминального клиента

Управление перенаправлением предусмотрено для локальных устройств следующих типов подключения:

- устройства, подключенные к последовательным (COM) портам;
- устройства, подключенные к параллельным (LPT) портам;
- подключенные диски;
- устройства Plug and Play.

По умолчанию перенаправление локальных устройств, подключаемых к компьютеру терминального клиента, не запрещается. В удаленных сеансах действуют параметры использования портов, дисков и других устройств Plug and Play, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для включения и отключения запрета перенаправления локальных устройств:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.

2. В разделе "Политики" перейдите к группе параметров "Контроль RDP-подключений".
3. Для параметра "Перенаправление устройств в RDP-подключениях" выберите нужное значение в раскрывающемся списке каждого типа подключения устройств:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование устройств в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные устройства к компьютеру" — блокирует использование устройств на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);
   - "Запрещено использовать устройства компьютера удаленно" — блокирует использование устройств на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
   - "Запрещено" — блокирует перенаправление устройств независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
   - "Определяется политиками Windows" — пользователи могут настраивать использование устройств в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.

   Примечание. Запрет перенаправления устройств Plug and Play поддерживается только на стороне терминального сервера ("Запрещено подключать удаленные устройства к компьютеру").
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Управление перенаправлением буфера обмена

По умолчанию перенаправление буфера обмена в терминальных подключениях не запрещается. В удаленных сеансах действуют параметры использования буфера обмена, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для включения и отключения запрета перенаправления буфера обмена:

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль RDP-подключений".
3. Для параметра "Перенаправление буфера обмена в RDP-подключениях" выберите нужное значение в раскрывающемся списке:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование буфера обмена в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные буферы обмена к компьютеру" — блокирует использование буфера обмена на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);

- "Запрещено использовать буфер обмена компьютера удаленно" — блокирует использование буфера обмена на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
- "Запрещено" — блокирует перенаправление буфера обмена независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
- "Определяется политиками Windows" — пользователи могут настраивать использование буфера обмена в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Управление перенаправлением принтеров

По умолчанию перенаправление принтеров, установленных на компьютере терминального клиента, не запрещается. В удаленных сеансах действуют параметры использования принтеров, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для включения и отключения запрета перенаправления принтеров:

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль RDP-подключений".
3. Для параметра "Перенаправление принтеров в RDP-подключениях" выберите нужное значение в раскрывающемся списке:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование принтеров в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные принтеры к компьютеру" — блокирует использование принтеров на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);
   - "Запрещено использовать принтеры компьютера удаленно" — блокирует использование принтеров на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
   - "Запрещено" — блокирует перенаправление принтеров независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
   - "Определяется политиками Windows" — пользователи могут настраивать использование принтеров в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Защита конфиденциальной информации при терминальных подключениях

В режиме контроля потоков механизма полномочного управления доступом можно включить автоматическое назначение уровня конфиденциальности для терминальных сессий. За счет этого будет обеспечиваться равенство уровней для сессий конфиденциальности на терминальном клиенте и на терминальном сервере.

Настройка параметров автоматического назначения уровней конфиденциальности для сессий пользователей выполняется при включении режима контроля потоков.

Глава 4
Настройка механизма самозащиты

Механизм самозащиты предназначен для предотвращения несанкционированных изменений конфигурации Secret Net Studio.

При включенном механизме самозащиты контролируются следующие операции с компонентами клиента Secret Net Studio:

- остановка критических служб и процессов;
- выгрузка драйверов;
- модификация или удаление ключей системного реестра;
- модификация или удаление файлов, в том числе от имени системной учетной записи;
- изменение прав доступа к файлам, папкам и ключам системного реестра.

Выполнение указанных операций с помощью средств администрирования ОС и специализированных утилит (например, Process Explorer и Kill Process) запрещается.

Выполнение операций, приведенных в списке выше, с помощью средств управления Secret Net Studio разрешается пользователям с соответствующей привилегией.

Важной функцией механизма самозащиты Secret Net Studio является контроль административных привилегий. Данная функция обеспечивает разграничение ролей администратора безопасности и локального администратора компьютера.

При включенном контроле административных привилегий осуществляется контроль доступа пользователей с правами локального администратора компьютера к следующим средствам управления Secret Net Studio:

- "Локальный центр управления";
- "Контроль программ и данных (централизованный режим)";
- "Контроль программ и данных";
- "Программа настройки подсистемы полномочного управления доступом";
- "Управление пользователями";
- программа установки клиента в режиме удаления;
- диалоговое окно "Управление Secret Net Studio" в Панели управления Windows.

Для получения доступа к данным средствам в режиме администрирования, а также для переключения механизма самозащиты в сервисный режим с помощью утилиты snsshell.exe (см. стр. **46**) необходимо указать PIN администратора безопасности.

События, связанные с функционированием механизма самозащиты, регистрируются в журнале Secret Net Studio.

Управление механизмом самозащиты может выполняться централизованно в Центре управления или непосредственно на защищаемом компьютере в Локальном центре управления. Управлять механизмом могут только следующие пользователи:

- для локального управления пользователь должен входить в локальную группу администраторов компьютера и в список учетных записей с привилегией на локальное управление механизмом самозащиты. По умолчанию в список включена локальная группа администраторов компьютера;

- для централизованного управления пользователь должен входить в группу администраторов домена безопасности и ему должны быть предоставлены привилегии "Администрирование системы защиты" и "Редактирование политик". По умолчанию эти привилегии предоставлены группе администраторов домена безопасности.

После установки клиента Secret Net Studio механизм самозащиты включен. Выполните настройку механизма в следующем порядке:

1. Добавьте пользователей, которые будут централизованно управлять механизмом самозащиты, в группу администраторов домена безопасности и предоставьте им нужные привилегии (см. раздел "Привилегии для работы с Центром управления" в документе [**1**]).
2. Настройте параметры механизма самозащиты (см. ниже).
3. Настройте параметры регистрации событий для механизма самозащиты (см. стр.**58**).

Настройка контроля административных привилегий

В этом разделе рассматривается процедура централизованной настройки параметров в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

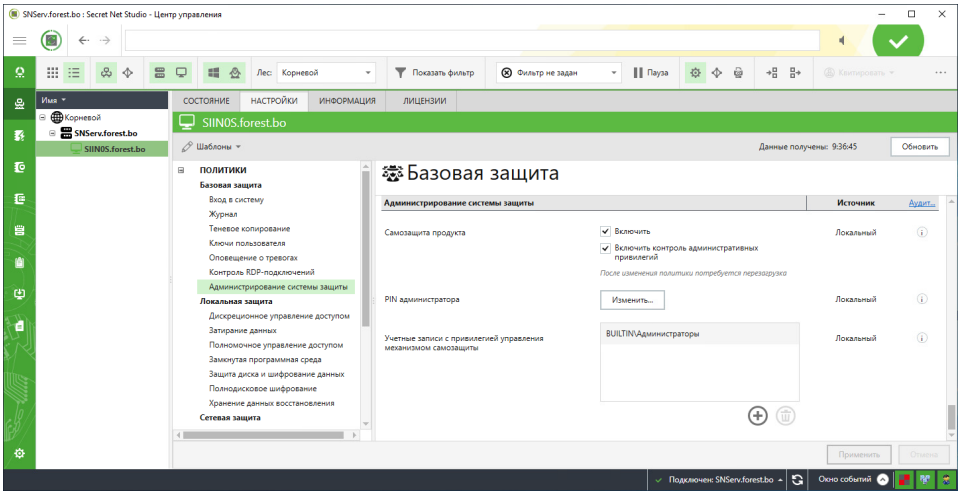
Для настройки контроля административных привилегий:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.

   Совет. Для настройки механизма непосредственно на защищаемом компьютере запустите Локальный центр управления, в панели "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Базовая защита | Администрирование системы защиты".

2. В разделе "Политики" перейдите к группе параметров "Базовая защита | Администрирование системы защиты".

   Пример содержимого группы параметров для компьютера представлен на рисунке ниже.



   Совет. Если выполняется настройка групповой политики, переведите выключатель слева от названия нужного параметра в положение "Вкл".

3. В поле "Включить контроль административных привилегий" настройте функцию, при использовании которой для запуска средств управления в режиме администрирования требуется указать PIN администратора:

- установите отметку, чтобы включить функцию. После этого на экране появится предупреждение о необходимости сменить PIN администратора. Для завершения операции нажмите кнопку "Да";
- удалите отметку, чтобы отключить функцию.

Пояснение. По умолчанию данная функция отключена. Функция может использоваться только при включенной самозащите.

4. В поле "PIN администратора" нажмите кнопку "Изменить", в появившемся диалоге введите новый PIN, введите его еще раз и нажмите кнопку "Применить".

Внимание! При вводе PIN учитывайте следующие требования и рекомендации.

- Длина PIN должна быть от 8 до 32 символов и он может содержать только следующие символы:
  - 1234567890 — цифры;
  - abcdefghijklmnopqrstuvwxyz — латинские буквы нижнего регистра (строчные);
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ — латинские буквы верхнего регистра (заглавные);
  - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — специальные символы.
- Следуйте следующим рекомендациям:
  - меняйте PIN с периодичностью, указанной в парольной политике;
  - используйте в PIN одновременно буквы, цифры и специальные символы.

5. В поле "Учетные записи с привилегией..." сформируйте список пользователей и групп, которым необходимо предоставить привилегию на локальное управление механизмом самозащиты. Для добавления и удаления учетных записей используйте кнопки под списком.

Внимание! Последний элемент из этого списка удалять запрещается.

6. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Отключение и включение самозащиты

Штатное отключение и повторное включение механизма самозащиты выполняется в Центре управления или Локальном центре управления. Эту операцию может выполнить только пользователь, обладающий необходимыми правами и привилегиями (см. стр.43). Для завершения операции необходимо перезагрузить компьютер.

Для отключения или включения самозащиты:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо выполнить операцию. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.

Совет. При работе непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", в панели "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Базовая защита | Администрирование системы защиты".

2. В разделе "Политики" перейдите к группе параметров "Базовая защита | Администрирование системы защиты".
3. Для параметра "Самозащита продукта" в поле "Включить":
   - удалите отметку, чтобы отключить механизм;
   - установите отметку, чтобы включить механизм.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".
5. Перезагрузите компьютеры, для которых была выполнена операция.

Переключение самозащиты в аварийный режим

Для экстренных случаев, когда использование штатных средств управления невозможно, но необходимо внести изменения в конфигурацию средств защиты, предусмотрена возможность переключения механизма самозащиты в аварийный режим.

Внимание! Используйте возможности аварийного режима только в экстренных ситуациях. Во всех остальных случаях пользуйтесь штатными средствами управления Secret Net Studio.

В аварийном режиме самозащита действует в ограниченном объеме. Разрешается модифицировать или удалять ключи системного реестра и файлы исполняемых модулей, относящиеся к компонентам клиента Secret Net Studio. Но при этом запрещается вносить несанкционированные изменения в конфигурацию средств защиты штатными локальными средствами управления. Например, удалять клиент целиком или его отдельные компоненты, переключать клиент из сетевого режима работы в автономный без наличия у пользователя привилегии на локальное управление механизмом самозащиты.

Для переключения в аварийный режим используется утилита командной строки snsshell.exe, находящаяся в каталоге установки клиента Secret Net Studio. Она позволяет включить аварийный режим при работе ОС Windows в защищенном или обычном режиме на время текущего сеанса работы. После перезагрузки компьютера самозащита вновь начинает работать в обычном режиме, но при этом за эталонную принимается текущая на этот момент конфигурация средств защиты.

Для переключения в аварийный режим:

1. Загрузите ОС Windows в защищенном (или обычном) режиме и войдите в систему с правами локального администратора компьютера.
2. В консоли командной строки перейдите в каталог установки клиента и выполните команду:

   ```
   snsshell.exe selfprot deactivatesd
   ```

   В окне консоли появится запрос PIN администратора.
3. Введите PIN администратора и нажмите клавишу <Enter>.

   Пояснение. По умолчанию после установки клиента Secret Net Studio PIN администратора имеет значение "12345678".

   При вводе правильного PIN самозащита будет переключена в аварийный режим. На экране появится подтверждающее сообщение. Также в сообщении будет предложено сменить PIN администратора.
4. Выполните нужные действия по изменению конфигурации средств защиты Secret Net Studio.

   Пояснение. Например, измените значение нужного ключа системного реестра, замените или переименуйте файл программного модуля, работа которого привела к неполадкам.
5. Перезагрузите компьютер.

Глава 5
Настройка теневого копирования

Общие сведения

Механизм теневого копирования предназначен для создания в системе дубликатов данных, выводимых на отчуждаемые носители информации. Дубликаты (копии) сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим теневого копирования.

Хранилище теневого копирования

В хранилище теневого копирования помещаются дубликаты (копии) данных, выводимых на отчуждаемые носители информации. Хранилище дубликатов представляет собой специально организованное место в системной папке на локальном диске компьютера.

Доступ к хранилищу теневого копирования осуществляется с учетом привилегий на управление журналами. Если пользователю предоставлены привилегии для просмотра журналов — пользователь получит доступ к хранилищу только для чтения. При наличии привилегий на управление журналами можно совершать административные операции с хранилищем.

Размер хранилища и методы его заполнения определяются заданными параметрами действующей политики безопасности.

Реализация поиска в хранилище теневого копирования

В Локальном центре управления предусмотрен поиск в хранилище теневого копирования. Функция поиска реализована с использованием компонента Windows Search, в котором для ускорения процесса поиска применяется индекс — база с подробными сведениями о файлах на компьютере. Формирование актуального индекса происходит при периодическом индексировании файлов. Запуск индексирования хранилища теневого копирования осуществляется автоматически в определенные моменты времени.

Новые файлы, помещаемые в хранилище теневого копирования, могут отсутствовать в индексе на момент поиска. Поэтому если поиск не дал результатов, это может быть связано с отсутствием новых файлов в индексе.

Особенности поиска по именам файлов

При сохранении дубликата в хранилище теневого копирования для файла генерируется новое внутреннее имя на основе его контрольной суммы и метки времени. Расширение файла не меняется, но может быть удалено при достижении ограничения на максимальную длину имени файла.

Имя файла дубликата в хранилище теневого копирования и исходное имя файла сопоставляются в записи о событии теневого копирования. Таким образом, по записи журнала можно восстановить файл в том виде, в каком был осуществлен его вывод на отчуждаемый носитель.

При поиске по именам файлов в хранилище теневого копирования используются внутренние, а не исходные имена файлов. Если требуется выполнить поиск по исходным именам файлов, следует воспользоваться средствами поиска по записям журнала Secret Net Studio — исходные имена файлов указаны в описаниях событий категории "Теневое копирование".

Особенности поиска по содержимому файлов

Компонент Windows Search, на базе которого реализован поиск в хранилище теневого копирования, по умолчанию поддерживает широкий спектр типов файлов для поиска по содержимому. Например, поиск по наличию слова или фразы выполняется в файлах с расширениями txt, htm, html, xml, а также в документах, сохраненных в приложениях пакета Microsoft Office.

Примечание. Полный перечень типов и форматов файлов, поддерживаемых компонентом Windows Search, приведен на сайте компании Microsoft.

Список типов и форматов файлов, поддерживаемых компонентом Windows Search для поиска по содержимому, расширяется при установке клиентского ПО системы Secret Net Studio.

Общий порядок настройки

Настройка механизма теневого копирования выполняется в следующем порядке:

1. Предоставьте пользователям, которые будут проводить аудит и администрировать хранилище теневого копирования, привилегии на просмотр и управление журналами (см. стр.**54**).
2. Настройте параметры хранилища теневого копирования для тех компьютеров, на которых будет использоваться теневое копирование (см. стр.**48**).
3. Определите на этих компьютерах устройства, для которых будет действовать теневое копирование (см. стр.**49**).
4. Периодически проводите аудит содержимого хранилища теневого копирования (см. стр.**50**).

Изменение параметров хранилища теневого копирования

При настройке параметров можно изменить ограничение максимального объема хранилища, а также включить или отключить возможность перезаписи.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки параметров хранилища:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Теневое копирование".
3. Для параметра "Размер хранилища" укажите нужный размер хранилища в процентах от дискового пространства.
4. Выберите вариант поведения системы при переполнении хранилища (если размер хранилища достигает максимального уровня):
   - чтобы разрешить вывод данных — установите отметку в поле "Автоматически перезаписывать старые данные при переполнении хранилища". В этом случае копии выводимых данных будут замещать наиболее старые копии, помещенные в хранилище;
   - чтобы запретить вывод данных — удалите отметку из поля. При достижении максимального размера хранилища новые попытки вывода данных будут блокироваться системой.
5. Настройте регистрацию событий, относящихся к работе механизма. Для перехода к соответствующей группе параметров регистрации используйте ссылку "Аудит" в правой части заголовка группы.
6. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка теневого копирования для устройств

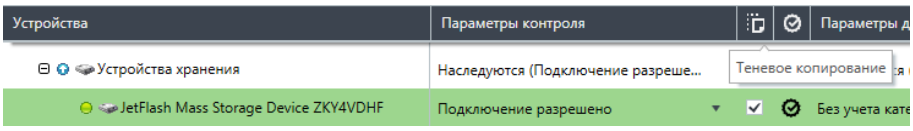
Функцию теневого копирования можно отключить для всех устройств или для всех принтеров. Если функция теневого копирования включена, будут действовать заданные параметры для устройств. Теневое копирование поддерживается для устройств следующих видов:

- устройства:
  - подключаемые сменные диски;
  - дисководы гибких дисков;
  - дисководы оптических дисков с функцией записи;
- принтеры.

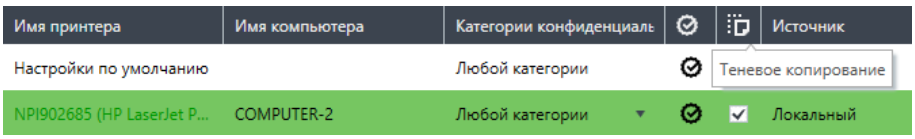
Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для управления функцией теневого копирования:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль устройств | Настройки" и для параметра "Теневое копирование" укажите нужное значение:
   - "Отключено для всех устройств" — теневое копирование при записи информации на устройства не выполняется;
   - "Определяется настройками устройства" — теневое копирование выполняется для устройств с включенным режимом теневого копирования.
3. В списке устройств выберите строку с нужным элементом списка и измените состояние выключателя в ячейке колонки "Теневое копирование":
   - установите отметку — чтобы включить режим сохранения копий;
   - удалите отметку — если нужно отключить этот режим.



4. В разделе "Политики" перейдите к группе параметров "Контроль печати | Настройки" и для параметра "Теневое копирование" укажите нужное значение:
   - "Отключено для всех принтеров" — теневое копирование при выводе на печать не выполняется;
   - "Определяется настройками принтера" — теневое копирование выполняется для принтеров с включенным режимом теневого копирования.
5. В списке принтеров выберите строку с нужным элементом списка и измените состояние выключателя в ячейке колонки "Теневое копирование":
   - установите отметку — чтобы включить режим сохранения копий;
   - удалите отметку — если нужно отключить этот режим.



Пояснение. Если устройства или принтеры не подключены к компьютеру, то в относящихся к ним строках списка нельзя поставить отметку в ячейке колонки "Теневое копирование".

6. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Поиск и просмотр данных в хранилище теневого копирования

Локальный центр управления позволяет настраивать параметры запроса для локального журнала. При загрузке записей с особыми критериями отбора могут использоваться запросы на поиск по файлам данных. Такие запросы предназначены для поиска файлов в хранилище теневого копирования и загрузки записей журнала, относящихся к этим файлам.

Для просмотра содержимого хранилища теневого копирования и выполнения стандартных операций с файлами (копирование, запуск, открытие и др.) используется программа "Проводник" ОС Windows. Вызов окна программы "Проводник" можно выполнить из Локального центра управления.

Внимание! При работе в программе "Проводник" блокируются все операции, связанные с удалением файлов из хранилища.

Предусмотрены следующие возможности для просмотра файлов в хранилище теневого копирования:

- открытие основной папки хранилища;
- открытие папки временных файлов, в которой предварительно создана копия выбранного файла с исходным именем.

Открытие основной папки хранилища

Основной папкой хранилища теневого копирования является корневая папка файловой структуры хранилища.

Для открытия окна с основной папкой хранилища:

1. В нижней части панели навигации (слева в основном окне Локального центра управления) нажмите кнопку "Настройки".

   На экране появится панель вызова средств настройки.
2. Выберите ссылку "Открыть папку теневого хранилища".

   На экране появится окно программы "Проводник" с содержимым основной папки хранилища.

Поиск и просмотр файлов

При регистрации событий теневого копирования дубликаты файлов, выводимых на отчуждаемые носители информации, помещаются в хранилище в особых служебных папках. Файлам дубликатов присваиваются внутренние имена, сгенерированные на основе контрольных сумм файлов и меток времени. В связи с этим переход к нужному файлу при просмотре содержимого хранилища может оказаться затруднительным.

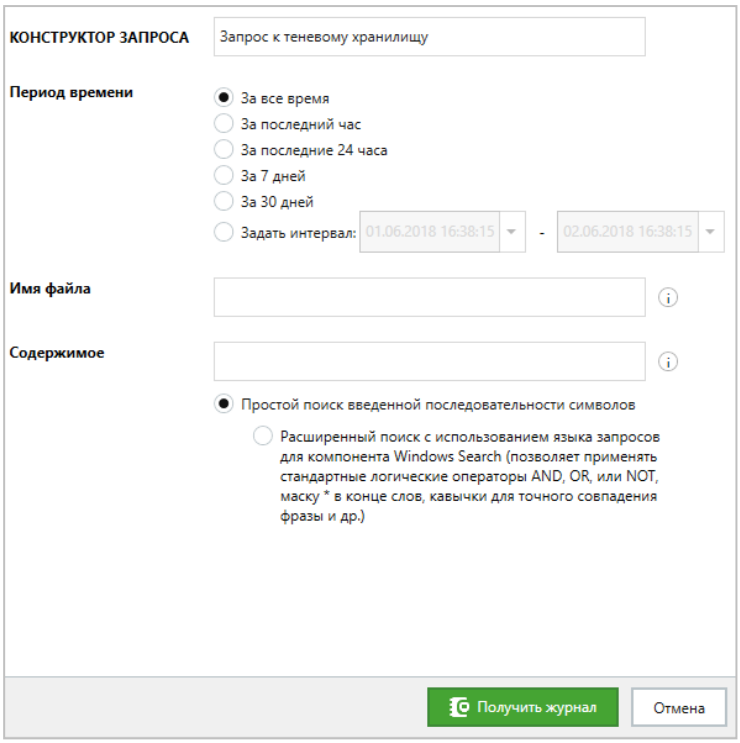
Локальный центр управления предоставляет возможность создать нужный файл с исходным именем и выполнить быстрый переход к этому файлу. Такой файл создается во временной папке хранилища на основе файла дубликата. Для создания используется запись журнала Secret Net Studio, содержащая сведения о событии теневого копирования с указанным исходным именем файла.

Внимание! Папка с временными файлами хранилища автоматически очищается при каждом запуске Локального центра управления.

Для настройки параметров запроса записей и просмотра временной копии файла в хранилище:

1. Загрузите Локальный центр управления и откройте панель "Журналы".
2. В панели управления запросами выберите команду "Новый | Запрос к теневому хранилищу".

На экране появится панель настройки параметров запроса.



3. В поле "Конструктор запроса" введите имя запроса.
4. Настройте параметры, приведенные в таблице ниже.

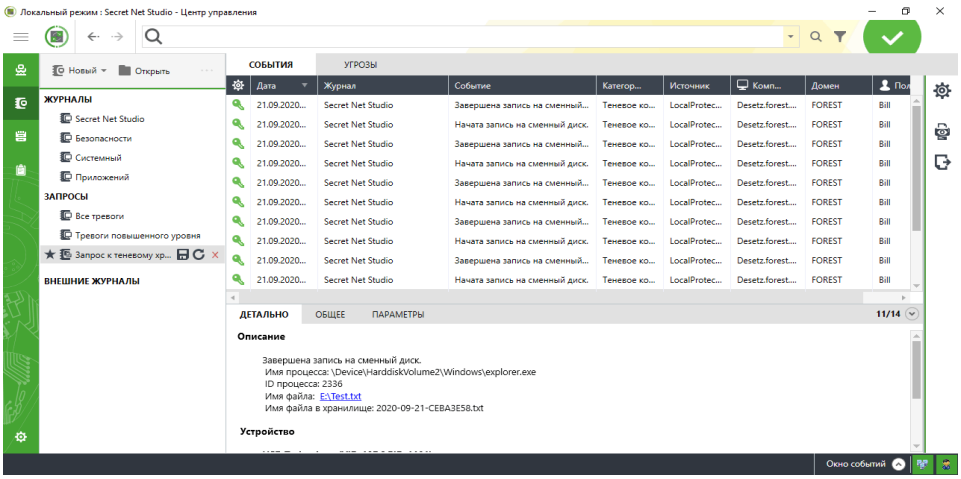
Группа полей "Период времени"
С помощью полей этой группы можно указать период для поиска записей журналов. Данный параметр может принимать одно из следующих значений: • "За все время"; • "За последний час"; • "За последние 24 часа"; • "За 7 дней"; • "За 30 дней"; • "Задать интервал" — укажите значение временного интервала
Имя файла
Определяет строку поиска в именах файлов. При поиске рассматриваются исходные имена файлов, содержащиеся в записях журнала Secret Net Studio (см. стр.**47**). Для поиска нескольких файлов можно указать несколько строковых значений, разделенных символом ";". Например, если требуется найти файлы, содержащие в своем названии сочетание букв "ОВ", в строке поиска можно указать: "ОВ*"; "*ОВ"; "*ОВ*"
Содержимое
Определяет строку поиска в содержимом файлов. Поиск по содержимому выполняется в файлах определенных типов и форматов, которые поддерживаются компонентом Windows Search (см. стр.**47**)
Переключатель для выбора простого или расширенного поиска
Если выбран простой поиск, введенные строки в полях "Имя файла" и "Содержимое" рассматриваются в том виде, как они указаны. То есть будут найдены файлы, в которых имя и/или содержимое включают указанный текст. В режиме простого поиска регистр символов не учитывается. В одном поле можно указать несколько строковых значений, разделенных запятой или символом ";". Если выбран расширенный поиск, введенные строки анализируются, и при наличии в них логических операторов или специальных символов поиск осуществляется в соответствии с правилами языка запросов для компонента Windows Search. В этом случае могут применяться логические операторы "И", "ИЛИ", "НЕ" (соответственно "AND", "OR" или "NOT"), маски для указания любых символов и другие средства. При расширенном поиске поисковые строки следует заключать в кавычки. Например, если требуется найти файлы, содержащие слова "секретный", "секретное", "секретные" и т. п. или фразу "конфиденциальный документ", в строке поиска можно указать: "секретн*" OR "конфиденциальный документ". Полный перечень возможностей языка запросов с примерами использования приводится на сайте компании Microsoft: http://msdn.microsoft.com/enus/ library/bb231270 (v=VS.85).aspx

5. Для применения заданных параметров нажмите кнопку "Получить журнал".

   Будет выполнен поиск нужных записей журнала и в области отображения сведений появится список найденных записей о событиях теневого копирования.

6. Выделите запись о событии теневого копирования, в которой содержатся данные о выводе файла на отчуждаемый носитель.

   В окне дополнительных сведений появится подробная информация о событии (см. рисунок ниже).



7. В окне дополнительных сведений выберите команду-ссылку, которая представлена в виде исходного имени файла в разделе "Описание".

Программа создаст копию файла с исходным именем во временной папке хранилища, после чего на экране появится окно программы "Проводник". В окне будет отображен список файлов временной папки с выделенным искомым файлом.

Глава 6
Локальный аудит

Локальные журналы регистрации событий

События, происходящие в системе, регистрируются в соответствующих журналах. Сведения о событиях сохраняются в виде записей, содержащих подробную информацию для анализа событий.

Журнал Secret Net Studio

В журнале событий системы Secret Net Studio (далее — журнал Secret Net Studio) накапливается информация о событиях, регистрируемых на компьютере средствами системы защиты.

Сведения, содержащиеся в журнале Secret Net Studio, позволяют контролировать работу механизмов защиты (защита входа в систему, контроль аппаратной конфигурации, контроль целостности и др.).

Состав регистрируемых событий определяется заданными параметрами действующей политики безопасности.

В журнале Secret Net Studio используется такой же формат данных и состав полей записей, как и в штатных журналах ОС Windows. Для локальной работы с записями журнала используется Локальный центр управления.

Штатные журналы ОС Windows

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. К штатным журналам относятся:

- журнал приложений — содержит сведения об ошибках, предупреждениях и других событиях, возникающих при работе приложений;
- системный журнал — содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;
- журнал безопасности — хранит информацию о доступе пользователей к компьютеру, применении групповых политик и изменении прав доступа, а также о событиях, связанных с использованием системных ресурсов.

Примечание. Описание содержимого штатных журналов ОС Windows и процедур настройки регистрации событий см. в документации к операционной системе.

Защитные подсистемы Secret Net Studio не осуществляют регистрацию событий в штатных журналах (за исключением журнала приложений, в котором могут регистрироваться некоторые специфические ошибки, связанные с функционированием ОС).

Локальный центр управления позволяет осуществлять загрузку и просмотр записей штатных журналов, хранящихся на компьютере локально. При этом сохраняется возможность загрузки записей в другие средства работы с журналами ОС Windows.

Привилегии для работы с локальными журналами

Доступ к записям журналов предоставляется сотрудникам, ответственным за управление системой защиты.

Для локальной работы с журналами предоставляются следующие привилегии:

- "Просмотр журнала системы защиты" — пользователь может загружать для просмотра записи локального журнала Secret Net Studio;

- "Управление журналом системы защиты" — пользователь может загружать для просмотра записи локального журнала Secret Net Studio, а также осуществлять его очистку.

  Примечание. Привилегия "Управление журналом системы защиты" включает в себя разрешение на просмотр журнала Secret Net Studio. Однако во всех случаях, когда пользователям требуется предоставить привилегию на управление журналом, рекомендуется предоставлять обе привилегии. Так, для обеспечения возможности просмотра копий теневого хранилища необходимо явно предоставить привилегию на просмотр журнала.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для предоставления привилегий:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Журнал".
3. Для параметров "Учетные записи с привилегией просмотра журнала системы защиты" и "Учетные записи с привилегией управления журналом системы защиты" отредактируйте списки пользователей и групп пользователей, которым предоставлены привилегии.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Хранение и очистка локальных журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы и хранятся на компьютере локально. Пока записи хранятся в локальном хранилище, их можно загрузить в Локальный центр управления или в другие программы, позволяющие осуществлять загрузку журналов (кроме журнала Secret Net Studio).

На клиентах в сетевом режиме функционирования локальные журналы хранятся в локальном хранилище до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов.

В автономном режиме функционирования журналы могут храниться только в локальном хранилище.

По мере регистрации событий записи журналов в локальном хранилище могут замещаться новыми записями. Перезапись информации в журналах осуществляется в соответствии с заданными параметрами регистрации событий.

В Центре управления пользователь может выполнять экспорт записей журналов в файлы. Если пользователю предоставлена соответствующая привилегия, он может выполнять и очистку журналов.

Экспорт записей локальных журналов

Локальный центр управления позволяет экспортировать (сохранять) в файлы записи локальных журналов. При экспорте предоставляется возможность очистки содержимого журнала после сохранения записей. Поддерживаемые форматы сохранения перечислены в следующей таблице.

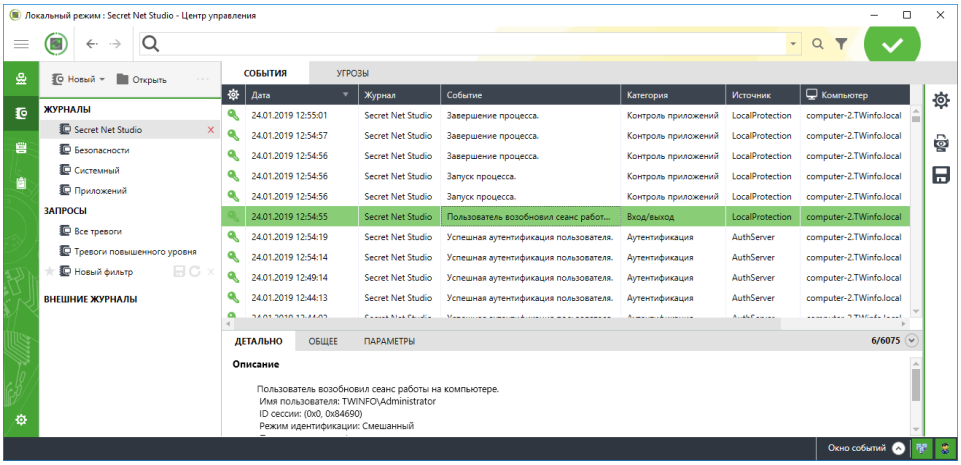
Имя	Формат	Описание
***.snlog**	Записи журнала станций системы Secret Net Studio	Загруженные в программу записи можно сохранить полностью или выборочно. Очистка журнала не осуществляется

Имя	Формат	Описание
***.evtx**	Стандартный формат журналов событий ОС Windows	В файле сохраняется все содержимое выбранного журнала (включая те записи, которые не загружены в программу). Экспорт журнала в данном формате может выполняться с последующей очисткой журнала после сохранения записей

Для экспорта записей:

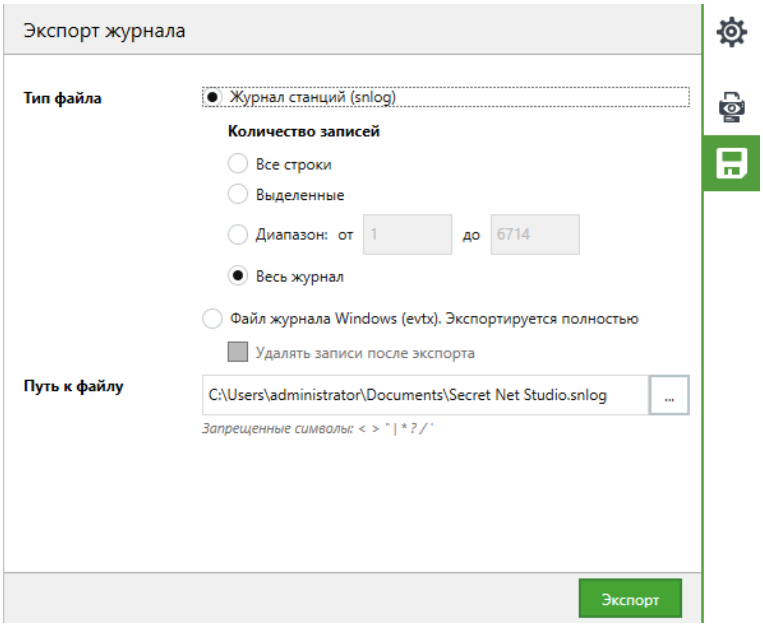
1. Загрузите в программу записи нужного журнала.

   Пример окна Локального центра управления с загруженными записями журнала Secret Net Studio представлен на следующем рисунке.



2. Если требуется экспортировать часть загруженных записей (при экспорте в snlog-файл), выделите нужные записи в таблице.
3. Нажмите кнопку "Экспорт журнала" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров экспорта.



4. В поле "Тип файла" выберите нужный формат экспорта.
5. В поле "Путь к файлу" введите полное имя файла для сохранения или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
6. Настройте параметры экспорта.

Группа полей "Количество записей"
Определяет, какие записи будут экспортированы в snlog-файл: • "Все строки" — выполняется экспорт записей, отображаемых в соответствии с текущими параметрами фильтрации; • "Выделенные" — выполняется экспорт только тех записей, которые выделены в таблице; • "Диапазон" — позволяет задать диапазон записей для экспорта по порядку их следования в таблице (в соответствии с текущими параметрами сортировки). Границы диапазона определяются в полях "от" и "до". Первая и последняя записи диапазона также будут экспортированы; • "Весь журнал" — выполняется экспорт всех записей, загруженных в запрос (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации)
Удалять записи после экспорта
Если установлена отметка, автоматически будет выполнена очистка журнала после экспорта записей в evtx-файл. Для очистки журнала Secret Net Studio пользователю должна быть предоставлена привилегия "Управление журналом системы защиты" (см. стр.**54**)

7. Нажмите кнопку "Экспорт".

Очистка локального журнала

Очистку (удаление записей) локального журнала можно выполнить при экспорте в evtx-файл (см. стр.**55**) или с помощью команды "Очистить журнал" в контекстном меню журнала (такая команда может применяться только для штатных журналов ОС Windows).

Настройка регистрации событий на компьютерах

Изменение параметров журнала Secret Net Studio

При настройке параметров можно изменить ограничение максимального объема журнала Secret Net Studio и политику перезаписи хранящейся информации.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки параметров журнала:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Журнал".
3. Для параметра "Максимальный размер журнала системы защиты" укажите значение максимально допустимого размера журнала в килобайтах. Диапазон значений — от 64 до 4 194 240 КБ (с шагом 64).
4. Для параметра "Политика перезаписи событий" выберите способ очистки журнала при его переполнении (если размер журнала достигает максимального значения). Для этого установите отметку в одном из полей, перечисленных ниже.

Затирать события по мере необходимости
При переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей
Затирать события старее <...> дней

При переполнении журнала система защиты автоматически удаляет записи, время хранения которых превысило заданный период. Новые записи не будут добавляться, если журнал достиг максимального размера и не содержит записей старше заданного периода. Диапазон ввода значений — от 1 до 365 дней
Не затирать события (очистка журнала вручную)
После достижения максимального размера записи хранятся в журнале. Новые события в журнале не регистрируются. Журнал можно очистить только вручную с помощью программы управления. Очистка должна выполняться периодически по мере накопления записей, чтобы не допустить переполнение журнала, так как это может привести к нарушениям в работе системы и вызвать блокировку компьютера

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Выбор событий, регистрируемых в журнале

По умолчанию в журнале Secret Net Studio регистрируются все возможные события, кроме некоторых событий категорий "Контроль приложений", "Контроль целостности" и "Дискреционный доступ".

Внимание! Часть событий регистрируется в обязательном порядке. Например, к таким событиям относятся события категории "Регистрация". Отключить регистрацию таких событий нельзя.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки списка регистрируемых событий:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. Выберите раздел "Регистрация событий".
3. Установите отметку в поле "Включить" для тех событий, которые необходимо регистрировать в журнале.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка контроля работы приложений

При работе приложений система Secret Net Studio может регистрировать события запуска и завершения исполняемых файлов процессов, а также операций доступа к данным процессов.

Для аудита отслеживания запуска и завершения процессов предусмотрены следующие варианты:

- регистрация событий для приложений, запуск которых выполняется пользователями;
- регистрация событий для всех процессов системы — не только пользовательских приложений, но и системных.

Примечание. Регистрация событий для всех процессов системы может существенно увеличить нагрузку на ядро Secret Net Studio и способствовать быстрому переполнению журнала записями о таких событиях. В большинстве случаев данный режим регистрации не является необходимым. Поэтому по умолчанию включена регистрация событий, относящихся только к пользовательским приложениям.

Попытки доступа к данным процессов контролируются, если включен режим изоляции процессов. Для корректного применения режим изоляции рекомендуется настраивать и использовать совместно с механизмом замкнутой программной среды. Описание процедур включения и настройки изоляции см. на стр.**125**.

Регистрацию событий разрешения и запрета можно включить для следующих операций с изолированными и неизолированными процессами:

- доступ к буферу обмена;
- доступ к содержимому окна процесса;
- перетаскивание данных между процессами методом drag-and-drop.

Настройка регистрации событий контроля работы приложений выполняется в Центре управления.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в Центре управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки контроля приложений:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Регистрация событий" перейдите к группе параметров "Контроль приложений".
3. Чтобы включить аудит отслеживания запуска и завершения для всех процессов системы, установите отметку для параметра "Аудит системных процессов (в дополнение к пользовательским)". Если достаточно регистрации только для приложений, запущенных пользователями, — удалите отметку.
4. В остальных параметрах группы "Контроль приложений" отметьте события, которые необходимо регистрировать в журнале.
5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Глава 7
Настройка механизма "Паспорт ПО"

Общие сведения

Механизм защиты "Паспорт ПО" предназначен для контроля состава и целостности ПО, установленного на защищаемых компьютерах. Контроль ПО осуществляется посредством сканирования исполняемых файлов и расчета их контрольных сумм. Совокупность контролируемых файлов на дисках компьютера представляет программную среду для сбора данных и анализа изменений.

Распознавание исполняемых файлов осуществляется по расширениям имен. Перечень расширений и каталоги поиска файлов можно настраивать. Сканирование может выполняться периодически по расписанию или в произвольные моменты времени по команде пользователя программы управления.

После сканирования полученные данные о СПС защищаемого компьютера загружаются на сервер безопасности и получают статус проекта паспорта для компьютера. Эти данные сравниваются с результатами предыдущего сканирования, которые хранятся в виде утвержденного паспорта. Изменения анализируются, и при необходимости проект паспорта утверждается в качестве текущего паспорта защищаемого компьютера.

Активация механизма

По умолчанию после установки ПО системы Secret Net Studio механизм "Паспорт ПО" не активирован. Активация механизма выполняется в следующем порядке:

1. Регистрация лицензий на использование механизма.
2. Включение механизма на защищаемых компьютерах.

Регистрация лицензий на использование механизма

Для механизма "Паспорт ПО" предусмотрена отдельная лицензия, которую необходимо зарегистрировать на защищаемых компьютерах. Добавление лицензии осуществляется в программе управления.

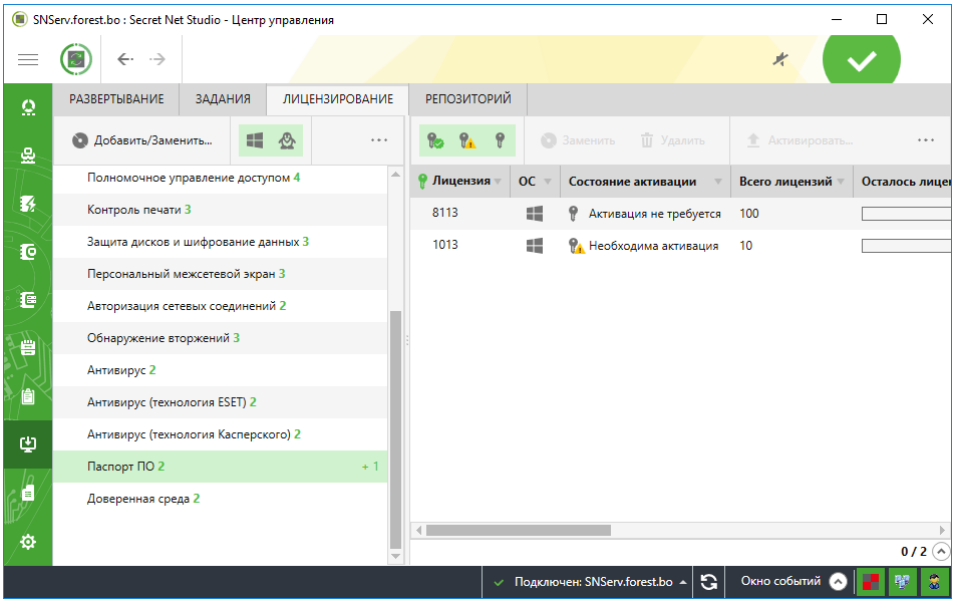
Лицензию можно зарегистрировать на рабочем месте администратора в централизованном режиме работы программы управления либо непосредственно на защищаемом компьютере в локальном режиме. Для клиентов в сетевом режиме функционирования рекомендуется регистрировать лицензию в централизованном хранилище, чтобы клиенты получали лицензии с сервера безопасности. Регистрация лицензии локально может потребоваться для компьютеров, не имеющих постоянной связи с сервером безопасности (например, с установленным клиентом в автономном режиме функционирования).

Регистрация лицензии в централизованном хранилище

Регистрация лицензий в централизованном хранилище выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает администратор безопасности (пользователь, входящий в группу администраторов домена безопасности).

Для регистрации лицензии в централизованном хранилище:

1. Откройте панель "Развертывание", перейдите на вкладку "Лицензирование" и нажмите кнопку "Добавить/Заменить".



2. В появившемся диалоге для выбора файла выберите нужный файл с лицензиями.
3. Если добавляемые лицензии требуют активации, выберите вариант активации лицензий и нажмите кнопку "Применить".

Примечание. Процедуры регистрации и активации лицензий являются одним из этапов процесса подготовки системы для централизованной установки ПО клиента Secret Net Studio. Этот метод установки является рекомендуемым. Дополнительные сведения о настройке и контроле централизованного развертывания ПО см. в документе[], глава 7.

Централизованная регистрация лицензии для компьютера

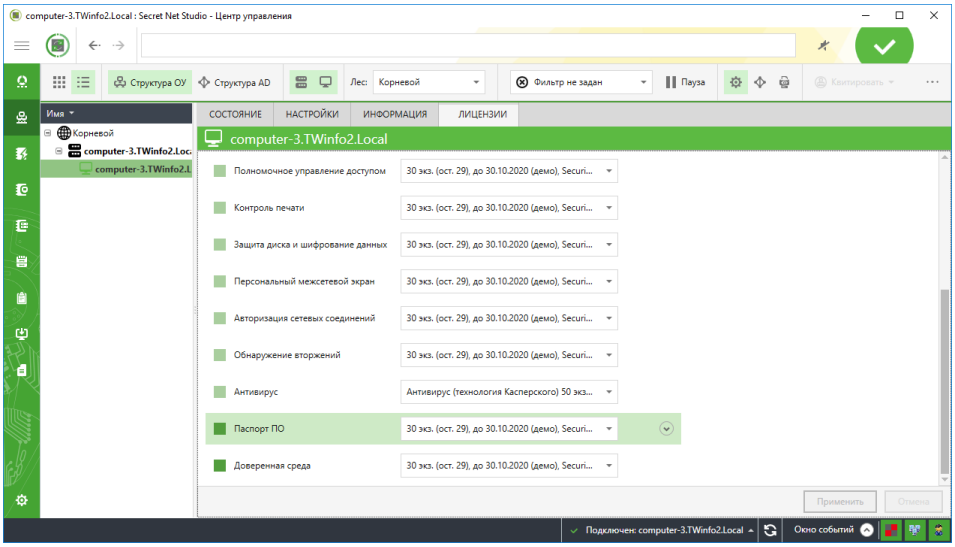
Если на клиенте Secret Net Studio в сетевом режиме функционирования отсутствует лицензия на использование механизма "Паспорт ПО", ее можно зарегистрировать для этого компьютера из числа доступных лицензий в централизованном хранилище. Такая операция может потребоваться, например, когда ПО клиента было установлено до регистрации лицензии в централизованном хранилище.

Примечание. Регистрация лицензии на компьютере выполняется автоматически, если ПО клиента было установлено централизованно после регистрации лицензии в централизованном хранилище.

Процедура централизованной регистрации лицензии выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает администратор безопасности (пользователь, входящий в группу администраторов домена безопасности).

Для централизованной регистрации лицензии на компьютере:

1. Откройте панель "Компьютеры", выберите нужный компьютер, вызовите его контекстное меню и выберите команду "Свойства". В появившейся панели свойств перейдите на вкладку "Лицензии".



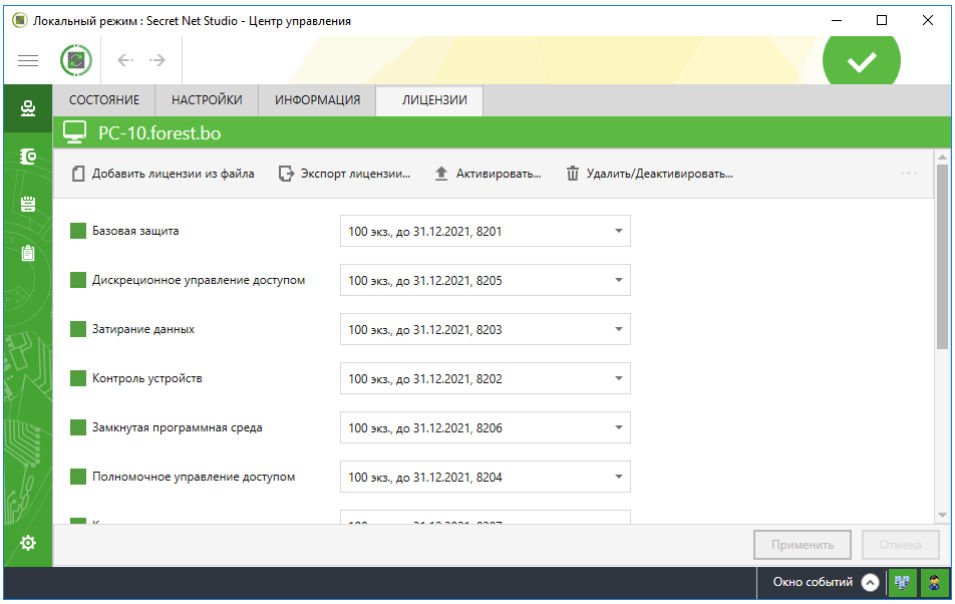
2. В списке защитных подсистем перейдите к элементу "Паспорт ПО". Отметьте элемент в поле слева и после загрузки сведений выберите лицензию в раскрывающемся списке. Чтобы отобразить информацию о выбранной лицензии, используйте кнопку справа.
3. Нажмите кнопку "Применить" в нижней части вкладки.

Регистрация лицензии локально на компьютере

Если защищаемый компьютер не имеет связи с сервером безопасности, регистрацию лицензии на использование механизма "Паспорт ПО" на данном компьютере можно выполнить локально. Процедура выполняется в локальном центре управления. Правами для выполнения операции обладает локальный администратор (пользователь, входящий в локальную группу администраторов).

Для локальной регистрации лицензии на компьютере:

1. Откройте панель "Компьютер", перейдите на вкладку "Лицензии" и нажмите кнопку "Добавить лицензии из файла".



2. В появившемся диалоге для выбора файла выберите нужный файл с лицензиями.

3. После загрузки лицензий из файла перейдите к элементу "Паспорт ПО" в списке защитных подсистем. Проверьте добавление лицензии для механизма. Элемент должен быть отмечен в поле слева, и в раскрывающемся списке должны присутствовать данные о лицензии. Чтобы отобразить информацию о лицензии, используйте кнопку справа.
4. Нажмите кнопку "Применить" в нижней части вкладки.

Включение механизма на защищаемых компьютерах

Включение механизма "Паспорт ПО" на защищаемых компьютерах может выполняться автоматически или вручную. Автоматическое включение происходит при централизованной установке клиента после регистрации лицензии в централизованном хранилище (по умолчанию в задании развертывания механизм отмечен для установки).

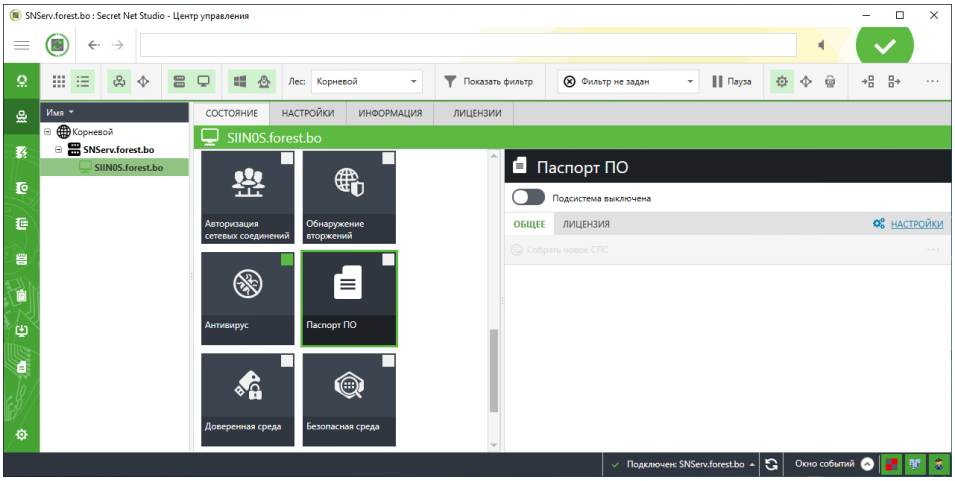
Если лицензия для механизма "Паспорт ПО" зарегистрирована на компьютере после установки клиента, включение механизма необходимо выполнить вручную централизованно или локально.

Централизованное включение механизма для компьютера

Процедура централизованного включения механизма выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает администратор безопасности (пользователь, входящий в группу администраторов домена безопасности).

Для централизованного включения механизма на компьютере:

1. Откройте панель "Компьютеры", выберите нужный компьютер, вызовите его контекстное меню и выберите команду "Свойства". В появившейся панели свойств на вкладке "Состояние" нажмите кнопку механизма "Паспорт ПО". Справа от кнопки появится блок, содержащий сведения о механизме.



2. Переведите в положение "Вкл" выключатель, расположенный слева в заголовке блока.

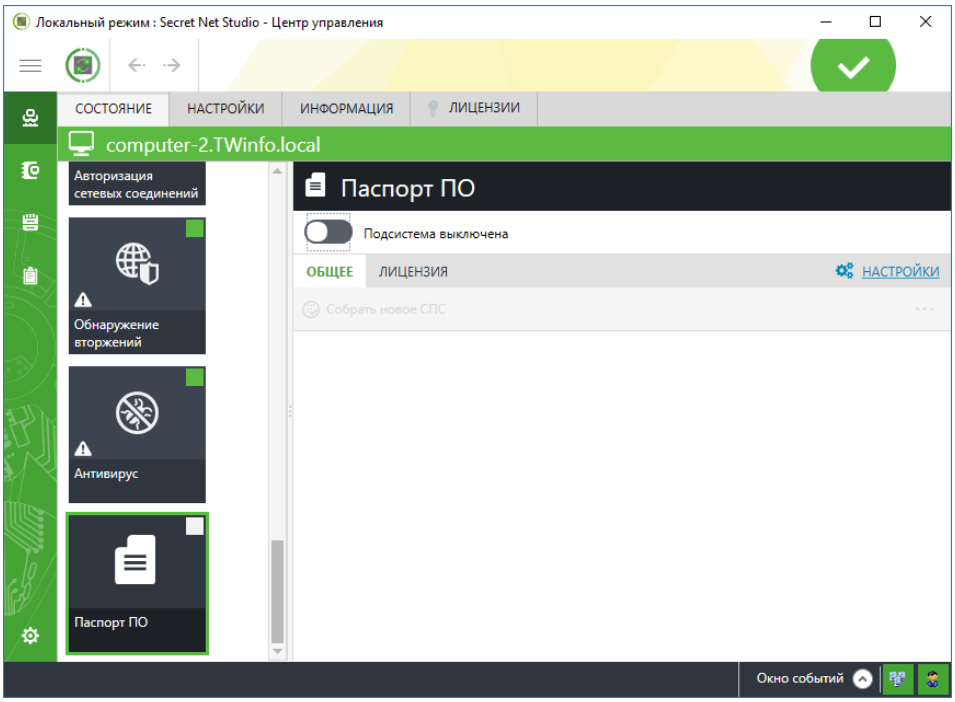
> **Примечание.** При первом включении механизма (когда на компьютере не установлены программные модули для его работы) для завершения процесса требуется перезагрузка компьютера. Чтобы удаленно инициировать перезагрузку, можно использовать соответствующую команду в контекстном меню компьютера или в меню "Команды" на панели инструментов программы.

Включение механизма локально на компьютере

Если защищаемый компьютер не имеет связи с сервером безопасности, включение механизма "Паспорт ПО" на данном компьютере можно выполнить локально. Процедура выполняется в Локальном центре управления. Правами для выполнения операции обладает локальный администратор (пользователь, входящий в локальную группу администраторов).

Для локального включения механизма на компьютере:

1. Откройте панель "Компьютер" и на вкладке "Состояние" нажмите кнопку механизма "Паспорт ПО". Справа от кнопки появится блок, содержащий сведения о механизме.



2. Переведите в положение "Вкл" выключатель, расположенный слева в заголовке блока.

Примечание. При первом включении механизма (когда на компьютере не установлены программные модули для его работы) для завершения процесса требуется перезагрузка компьютера.

Настройка механизма

Настройка механизма "Паспорт ПО" выполняется в следующем порядке:

1. Генерация ключевой информации для утверждения паспортов ПО.
2. Предоставление привилегий пользователям.
3. Редактирование структуры ОУ.
4. Настройка параметров функционирования механизма.

Генерация ключевой информации для утверждения паспортов ПО

Для утверждения проектов паспортов пользователю требуется использовать ключевую информацию, сгенерированную в Secret Net Studio. Ключевую информацию составляют криптографические ключи (открытый и закрытый), которые также могут применяться в механизме шифрования данных в криптоконтейнерах. Открытый ключ хранится в базе данных Secret Net Studio, закрытый — на ключевом носителе пользователя.

Ключевая информация генерируется в программе управления пользователями. Криптографические ключи можно создать во время присвоения пользователю идентификатора или позже. Описание процедуры присвоения идентификатора см. на стр.**31**. Чтобы создать криптографические ключи, в мастере присвоения идентификатора нужно включить параметр "Записать в идентификатор закрытый ключ пользователя". Если нужно сгенерировать ключевую информацию после присвоения идентификатора, администратор может выполнить процедуру выдачи/смены ключей при управлении криптографическими ключами (см. стр.**201**).

Предоставление привилегий пользователям

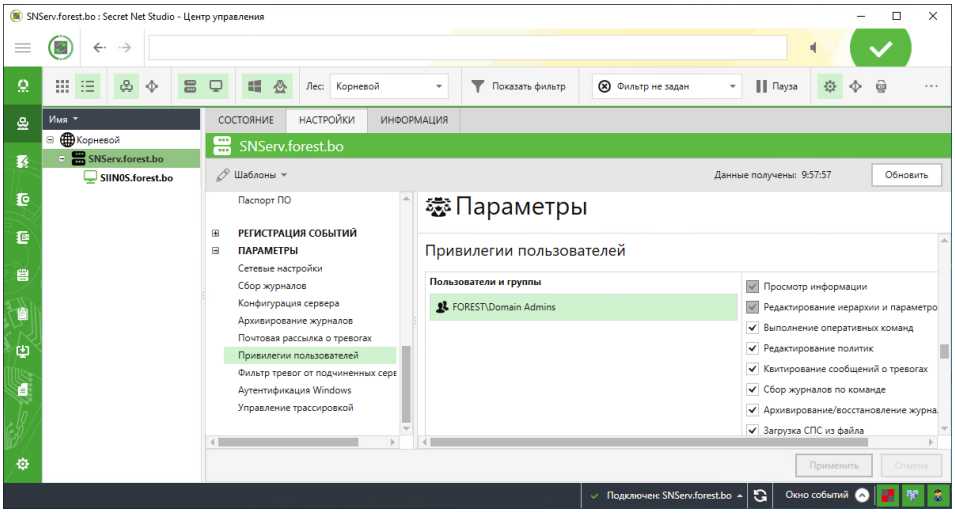
Права на управление механизмом "Паспорт ПО" можно распределить между сотрудниками в соответствии с ролями, указанными в следующей таблице.

Роль	Функции
Администратор (пользователь, являющийся членом группы администраторов домена безопасности)	• Назначает необходимые привилегии для остальных ролей. • Активирует механизм "Паспорт ПО" на защищаемых компьютерах (включает действие механизма). • Настраивает параметры группы "Паспорт ПО" в политиках объектов управления (расписание сканирования, список расширений файлов и каталогов для контроля, регистрацию событий). • Загружает журналы для просмотра сведений о событиях, связанных с работой механизма. • Запускает синхронизацию базы данных паспортов на сервере безопасности. • Удаляет устаревшие паспорта
Контролер	• Импортирует СПС защищаемых компьютеров в БД СБ. • Утверждает проекты паспортов (заверяет электронной подписью). • Запускает сканирование и сбор СПС из программы управления в централизованном режиме
Оператор	• Запускает сканирование и сбор СПС из Локального центра управления (для автономной версии). • Сохраняет полученные СПС в файлы (для автономной версии). • Загружает для просмотра и сравнивает содержимое паспортов в программе управления в централизованном режиме

Предоставление привилегий выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает администратор безопасности (пользователь, входящий в группу администраторов домена безопасности).

Для предоставления привилегий:

1. В панели "Компьютеры" вызовите контекстное меню сервера безопасности и выберите команду "Свойства". В появившейся панели свойств перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки".
2. В левой части вкладки "Настройки" перейдите к разделу "Параметры" и выберите группу "Привилегии пользователей".



3. В список "Пользователи и группы" добавьте учетные записи пользователей, для которых нужно назначить роли контролера и оператора. Для этого нажмите кнопку "Добавить пользователя" (под списком "Пользователи и группы") и выберите нужные учетные записи в стандартном диалоге выбора объектов.

   Примечание. При необходимости удалить добавленную учетную запись выберите ее в списке и нажмите кнопку "Удалить пользователя".

4. Для пользователей, которым назначается роль контролера, отметьте привилегии "Выполнение оперативных команд", "Загрузка СПС из файла" и "Утверждение паспорта ПО".

   Примечание. Оператору для работы с программой управления в централизованном режиме достаточно привилегии "Просмотр информации", предоставляемой по умолчанию. Для работы с Локальным центром управления пользователь должен быть членом локальной группы администраторов компьютера.

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Редактирование структуры ОУ

Для обработки и анализа данных о состоянии программной среды защищаемых компьютеров эти компьютеры должны быть представлены в структуре ОУ. При установке клиента Secret Net Studio с подчинением серверу безопасности компьютер автоматически добавляется в структуру ОУ. Если клиент был установлен без подчинения серверу безопасности, необходимо выполнить соответствующие операции добавления компьютера в структуру и подчинения соответствующему СБ. Действия выполняются в Центре управления в централизованном режиме работы (см. документ [**1**], раздел "Редактирование структуры ОУ").

Примечание. В структуре ОУ должны быть представлены все компьютеры, на которых будет выполняться сбор данных для механизма "Паспорт ПО". Даже те, которые не имеют постоянной связи с сервером безопасности (например, компьютеры с установленным клиентом в автономном режиме функционирования). Для добавления компьютера в структуру ОУ достаточно, чтобы соответствующий ему объект присутствовал в структуре Active Directory. Если объект отсутствует (компьютер не подключен к домену AD), создайте его вручную с тем же именем в стандартной оснастке управления пользователями и компьютерами Active Directory.

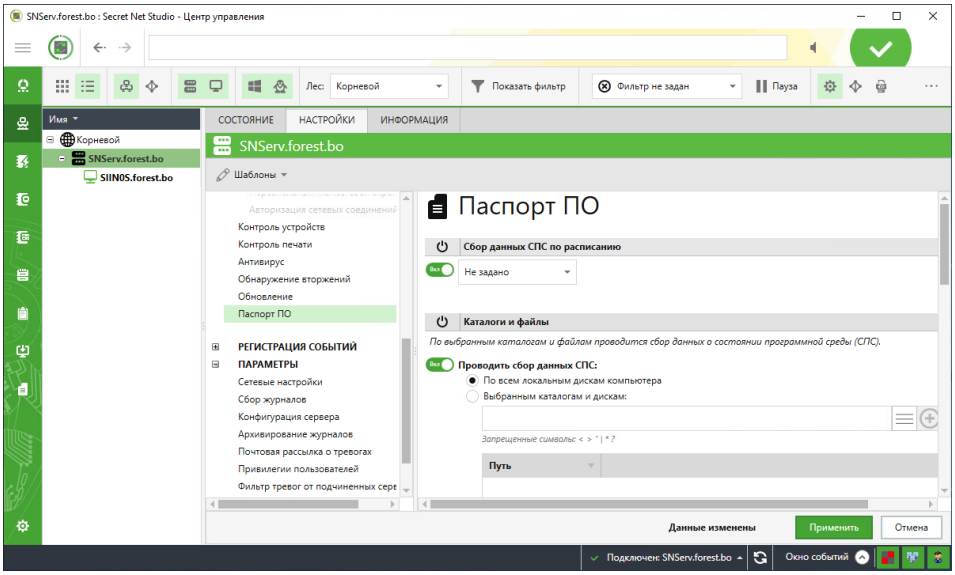
Централизованная настройка параметров механизма

Процедура централизованной настройки параметров механизма "Паспорт ПО" выполняется в программе управления в централизованном режиме работы. Параметры могут быть заданы непосредственно для защищаемого компьютера (параметры локальной политики), а также для доменов, организационных подразделений и серверов безопасности. Применение параметров осуществляется по тем же принципам, как и для других механизмов: наименьший приоритет имеют параметры локальной политики, наивысший — параметры, заданные для корневого сервера безопасности.

Правами для централизованной настройки параметров обладает администратор безопасности (пользователь, входящий в группу администраторов домена безопасности).

Для настройки параметров механизма:

1. Откройте панель "Компьютеры", вызовите контекстное меню нужного объекта и выберите команду "Свойства". В появившейся панели свойств перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки".
2. В левой части вкладки "Настройки" перейдите к разделу "Политики" и выберите группу "Паспорт ПО".



Примечание. В политиках домена, организационного подразделения или сервера безопасности применяются только явно заданные параметры. Чтобы задать значения параметров, используйте выключатели слева от параметра — выключатель необходимо перевести в положение "Вкл".

3. Если запуск процесса сбора данных о состоянии программной среды должен выполняться в определенные моменты времени, настройте расписание запуска. Для этого выберите нужный режим в раскрывающемся списке группы параметров "Сбор данных СПС по расписанию".

Периодическое
Запуск процесса сбора данных осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения

Еженедельное
Запуск процесса сбора данных осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

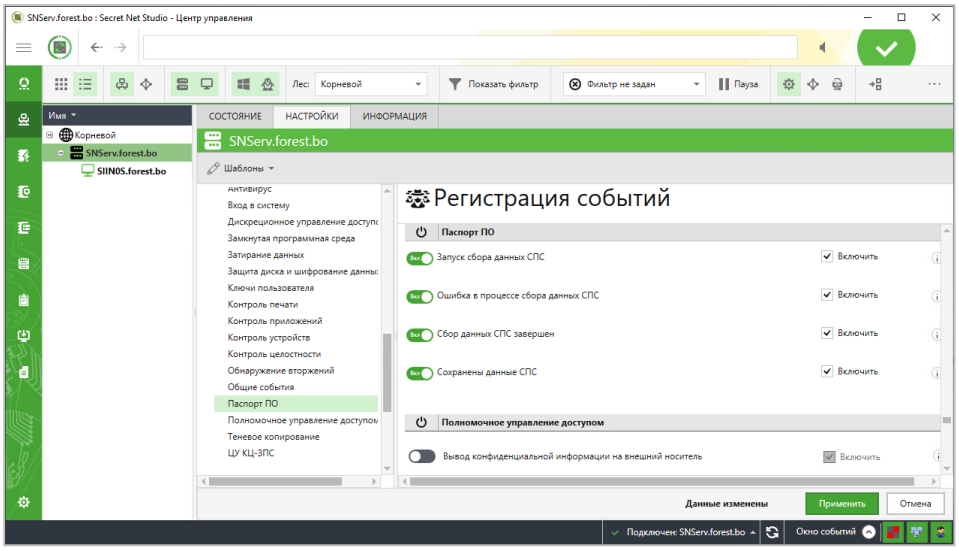
4. В группе параметров "Каталоги и файлы" настройте область сканирования при сборе данных. Для этого установите отметки в соответствующих полях.

По всем локальным дискам компьютера
При сборе данных сканирование будет выполняться во всех каталогах на всех локальных дисках компьютера, кроме указанных в списке исключений
Выбранным каталогам и дискам
При сборе данных сканирование будет выполняться только в каталогах, указанных в списке. Чтобы добавить каталог в список, введите полный путь (с указанием диска) в строке ввода и нажмите справа кнопку "Добавить". Путь можно указать с использованием общесистемной переменной окружения (например, %ProgramFiles%). Для выбора переменной нажмите кнопку "Добавить из списка по умолчанию", которая расположена в строке ввода рядом с кнопкой "Добавить". Для редактирования и удаления элементов в списке используйте соответствующие кнопки, расположенные под списком
Исключить каталоги, диски и файлы
При сборе данных будут пропущены каталоги и файлы, указанные в списке. Список путей к каталогам и файлам исключений формируется аналогично списку сканирования по выбранным каталогам и файлам

5. В группе параметров "Расширения файлов" укажите расширения имен файлов для сканирования. Для этого установите отметки в соответствующих полях.

По всем расширениям файлов
При сборе данных сканирование будет выполняться для всех обнаруженных файлов
Выбранным
При сборе данных сканирование будет выполняться только для файлов с расширениями, указанными в списке. Чтобы добавить расширение в список, введите его в строке ввода и нажмите справа кнопку "Добавить". Можно указать расширение из списка стандартных расширений исполняемых файлов — для этого нажмите кнопку "Добавить из списка по умолчанию", которая расположена в строке ввода рядом с кнопкой "Добавить". Для редактирования и удаления элементов в списке используйте соответствующие кнопки, расположенные под списком

6. В левой части вкладки "Настройки" перейдите к разделу "Регистрация событий" и выберите группу "Паспорт ПО".



Примечание. В политиках домена, организационного подразделения или сервера безопасности применяются только явно заданные параметры. Чтобы задать значения параметров, используйте выключатели слева от каждого параметра — выключатель необходимо перевести в положение "Вкл".

7. Включите регистрацию нужных событий в локальных журналах защищаемых компьютеров. Для этого установите отметки в соответствующих полях.

Запуск сбора данных СПС
Событие регистрируется при запуске процесса сбора данных о СПС
Ошибка в процессе сбора данных СПС
Событие регистрируется при возникновении ошибки во время сбора данных (например, из-за сбоя при доступе к файловому объекту при сканировании)
Сбор данных СПС завершен
Событие регистрируется после завершения процесса сбора данных о СПС
Сохранены данные СПС
Событие регистрируется при сохранении СПС в отдельном файле (локально на защищаемом компьютере) или при передаче СПС на сервер безопасности

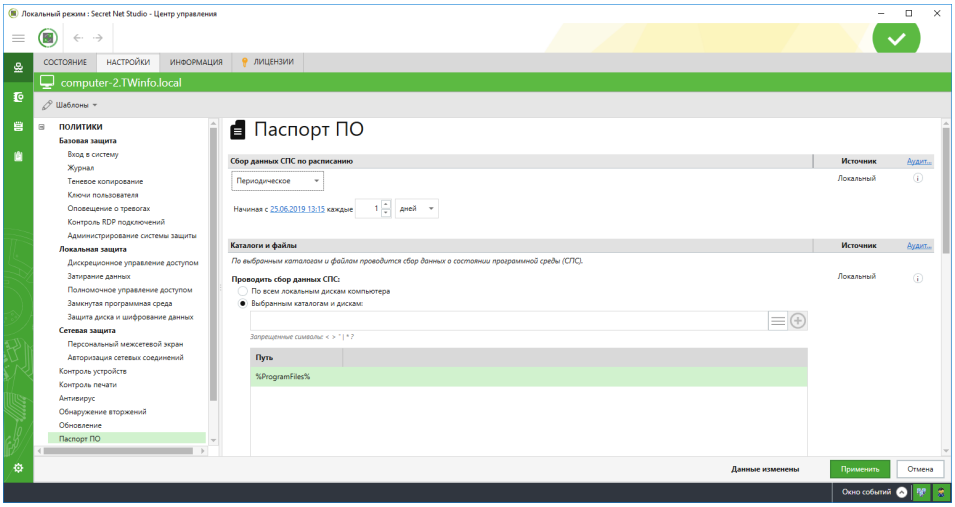
8. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка параметров механизма локально на компьютере

Если защищаемый компьютер не имеет связи с сервером безопасности, настройку параметров механизма "Паспорт ПО" на данном компьютере можно выполнить локально. Процедура выполняется в Локальном центре управления. Правами для выполнения действий обладает локальный администратор (пользователь, входящий в локальную группу администраторов).

Для локальной настройки параметров механизма на компьютере:

1. Откройте панель "Компьютер", перейдите на вкладку "Настройки" и в разделе "Политики" (в левой части вкладки) выберите группу "Паспорт ПО".



Примечание. Параметры локальной политики недоступны для редактирования, если они явно заданы в политиках домена, организационного подразделения или сервера безопасности. Редактировать можно только те параметры, у которых в колонке "Источник" указан статус "Локальный".

2. Если запуск процесса сбора данных о состоянии программной среды должен выполняться в определенные моменты времени, настройте расписание запуска. Для этого выберите нужный режим в раскрывающемся списке группы параметров "Сбор данных СПС по расписанию".

Периодическое
Запуск процесса сбора данных осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения
Еженедельное
Запуск процесса сбора данных осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

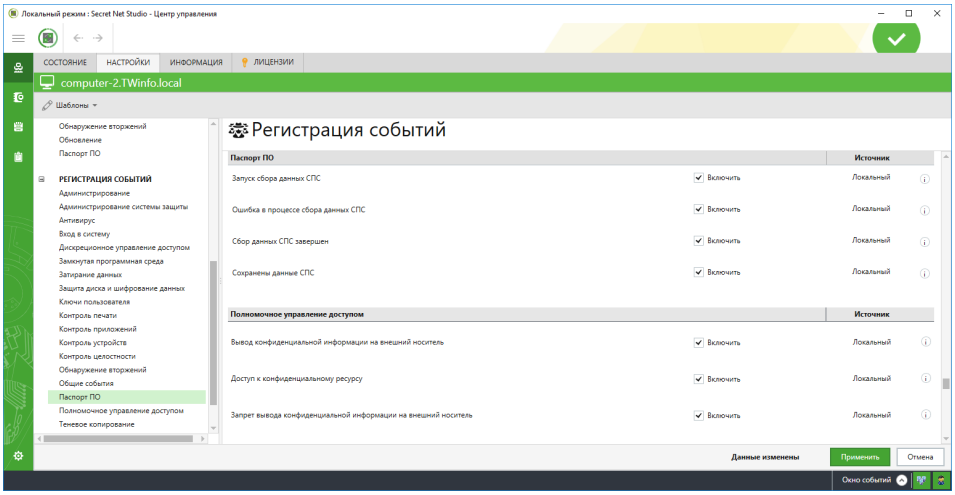
3. В группе параметров "Каталоги и файлы" настройте область сканирования при сборе данных. Для этого установите отметки в соответствующих полях.

По всем локальным дискам компьютера
При сборе данных сканирование будет выполняться во всех каталогах на всех локальных дисках компьютера, кроме указанных в списке исключений
Выбранным каталогам и дискам
При сборе данных сканирование будет выполняться только в заданных каталогах. Чтобы добавить каталог в список, введите полный путь (с указанием диска) в строке ввода и нажмите справа кнопку "Добавить". Путь можно указать с использованием общесистемной переменной окружения (например, %ProgramFiles%). Для выбора переменной нажмите кнопку "Добавить из списка по умолчанию", которая расположена в строке ввода рядом с кнопкой "Добавить". Для редактирования и удаления элементов в списке используйте соответствующие кнопки, расположенные под списком
Исключить каталоги, диски и файлы
При сборе данных будут пропущены каталоги и файлы, указанные в списке. Список путей к каталогам исключений формируется аналогично списку сканирования по выбранным каталогам и файлам

4. В группе параметров "Расширения файлов" укажите расширения имен файлов для сканирования. Для этого установите отметки в соответствующих полях.

По всем расширениям файлов
При сборе данных сканирование будет выполняться для всех обнаруженных файлов
Выбранным
При сборе данных сканирование будет выполняться только для файлов с расширениями, указанными в списке. Чтобы добавить расширение в список, введите его в строке ввода и нажмите справа кнопку "Добавить". Можно указать расширение из списка стандартных расширений исполняемых файлов — для этого нажмите кнопку "Добавить из списка по умолчанию", которая расположена в строке ввода рядом с кнопкой "Добавить". Для редактирования и удаления элементов в списке используйте соответствующие кнопки, расположенные под списком

5. В левой части вкладки "Настройки" перейдите к разделу "Регистрация событий" и выберите группу "Паспорт ПО".



Примечание. Параметры локальной политики недоступны для редактирования, если они явно заданы в политиках домена, организационного подразделения или сервера безопасности. Редактировать можно только те параметры, у которых в колонке "Источник" указан статус "Локальный".

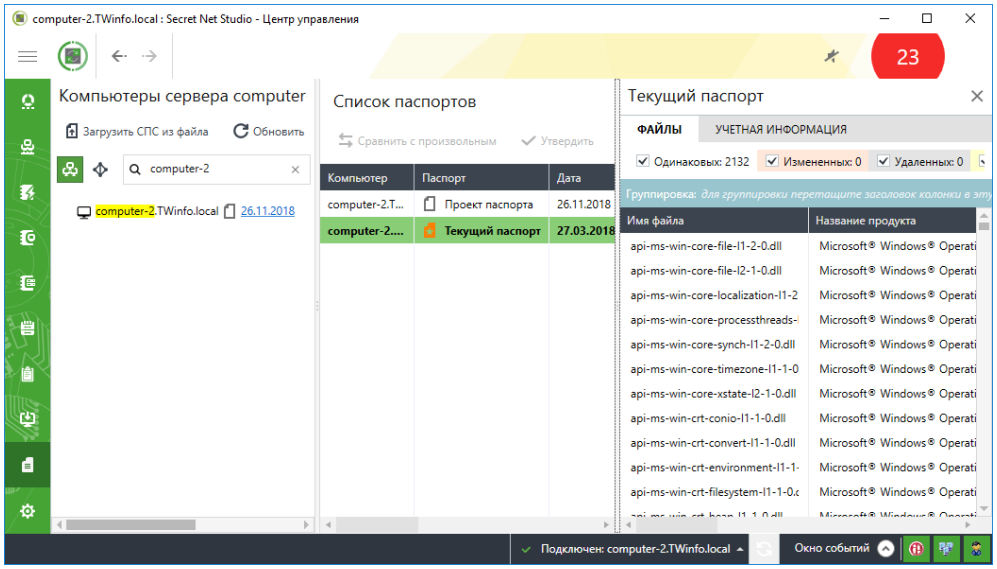
6. Включите регистрацию нужных событий в локальном журнале. Для этого установите отметки в соответствующих полях.

Запуск сбора данных СПС
Событие регистрируется при запуске процесса сбора данных о СПС
Ошибка в процессе сбора данных СПС
Событие регистрируется при возникновении ошибки во время сбора данных (например, из-за сбоя при доступе к файловому объекту при сканировании)
Сбор данных СПС завершен
Событие регистрируется после завершения процесса сбора данных о СПС
Сохранены данные СПС
Событие регистрируется при сохранении СПС в отдельном файле (локально на защищаемом компьютере) или при передаче СПС на сервер безопасности

7. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Работа с паспортами

Обработка паспортов ПО осуществляется в программе управления в централизованном режиме работы. Действия выполняются в специальной панели управления, которая загружается при выборе ярлыка "Паспорт ПО" в панели навигации. Пример содержимого панели представлен на следующем рисунке.



Общая последовательность процедур проверки и получения паспорта защищаемого компьютера:

1. Сбор данных о СПС на защищаемом компьютере.
2. Создание проекта паспорта (загрузка полученных данных о СПС в БД сервера безопасности).
3. Сравнение проекта паспорта и имеющихся паспортов для компьютера.
4. Проверка действительности подписи для утвержденных паспортов.
5. Утверждение проекта паспорта в качестве текущего паспорта.

Для обслуживания базы паспортов предусмотрены следующие возможности:

- резервное копирование;
- удаление неактуальных паспортов;
- восстановление паспортов из резервного хранилища;
- экспорт паспортов в файл.

Сбор данных о СПС на защищаемом компьютере

На защищаемых компьютерах сбор данных о состоянии программной среды может выполняться в соответствии с настроенным расписанием (см. выше), а также по команде из программы управления. Запуск процесса сбора данных на компьютере можно выполнить централизованно или локально.

Централизованный запуск сбора данных

Централизованный запуск сбора данных о СПС для защищаемого компьютера выполняется в программе управления в централизованном режиме работы. Правами для централизованного запуска обладает пользователь с привилегиями "Выполнение оперативных команд" и "Загрузка СПС из файла".

Для централизованного запуска сбора данных:

1. В левой части панели "Паспорт ПО" выберите нужный компьютер. При необходимости для быстрого перехода к компьютеру используйте средства фильтрации и поиска, расположенные над списком объектов.

2. Вызовите контекстное меню компьютера и выберите команду "Собрать новое СПС". На компьютере начнется сбор данных, и до завершения процесса в строке с именем компьютера отображается соответствующий статус. По окончании процесса появится ссылка "загрузить".

Запуск сбора данных локально на компьютере

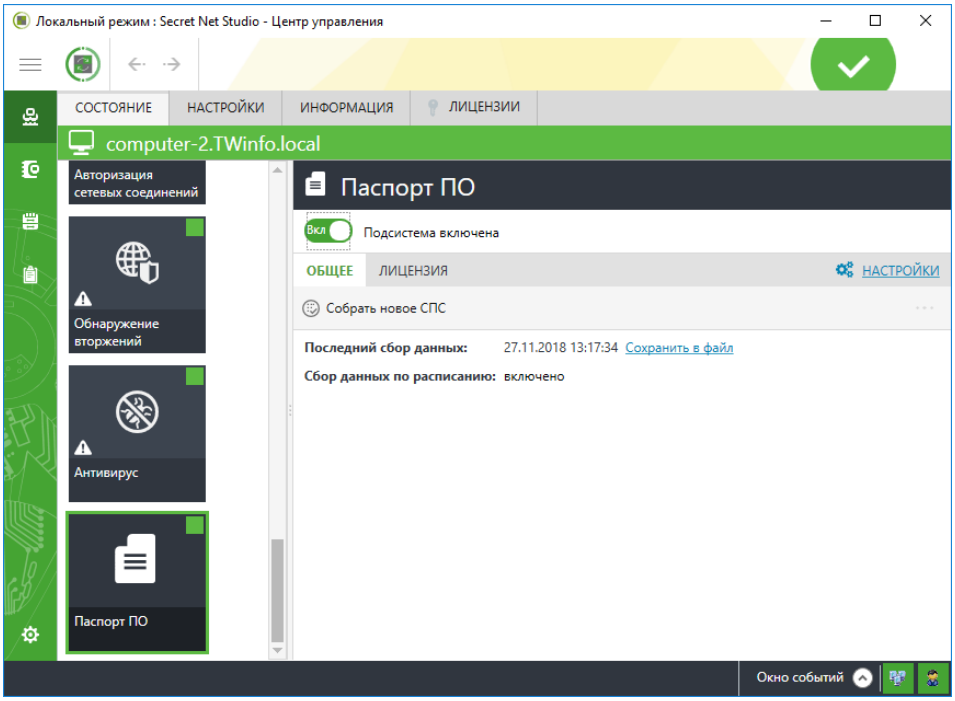
Если защищаемый компьютер не имеет связи с сервером безопасности, запуск сбора данных о СПС на данном компьютере можно выполнить локально. При этом если компьютер не будет доступен по сети к моменту создания проекта паспорта — необходимо создать специальный файл, с помощью которого можно будет загрузить данные в БД сервера безопасности.

Процедура локального сбора данных выполняется в программе управления в локальном режиме работы. Правами для выполнения действий обладает локальный администратор (пользователь, входящий в локальную группу администраторов).

Для локального запуска сбора данных на компьютере:

1. Откройте панель "Компьютер" и на вкладке "Состояние" нажмите кнопку механизма "Паспорт ПО".

   Справа от кнопки появится блок, содержащий сведения о механизме.



Примечание. Проверьте сведения о времени предыдущего сбора данных, указанные в строке "Последний сбор данных". Если ранее полученные данные актуальны на текущий момент (например, от недавнего сбора данных по расписанию) — можно не выполнять новый сбор данных и перейти к выполнению действия 3.

2. Для запуска сбора данных нажмите кнопку "Собрать новое СПС" под заголовком блока.

   На компьютере начнется сбор данных, и до завершения процесса в блоке отображается соответствующий статус. По окончании процесса будут обновлены сведения о последнем сборе данных и появится ссылка "Сохранить в файл".

3. При необходимости сохраните полученные данные в файле для последующей загрузки в БД сервера безопасности. Для этого выберите ссылку "Сохранить в файл" и укажите размещение в появившемся диалоге сохранения файла.

Создание проекта паспорта

При загрузке данных о СПС в БД сервера безопасности в списке паспортов защищаемого компьютера создается новый проект паспорта. Если в списке присутствует ранее созданный проект, после загрузки данных он будет замещен новым проектом паспорта.

Процедура загрузки данных о СПС выполняется в программе управления в централизованном режиме работы. Загрузка может выполняться непосредственно с защищаемого компьютера или из файла, созданного при локальном сборе данных. Правами для загрузки данных обладает пользователь с привилегиями "Выполнение оперативных команд" и "Загрузка СПС из файла".

Для загрузки данных и создания проекта паспорта:

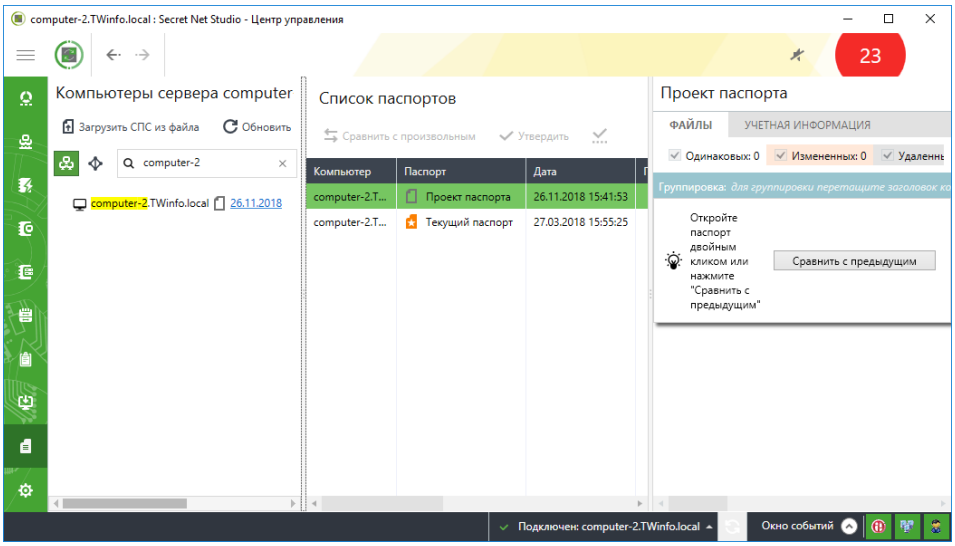
1. В левой части панели "Паспорт ПО" выберите нужный компьютер. При необходимости для быстрого перехода к компьютеру используйте средства фильтрации и поиска, расположенные над списком объектов.
2. Вызовите контекстное меню компьютера и выберите нужную команду:
   - "Загрузить последнее СПС" — чтобы загрузить данные непосредственно с защищаемого компьютера (компьютер должен быть включен и доступен по сети);
   - "Загрузить СПС из файла" — чтобы загрузить данные из файла, созданного при локальном сборе данных.
3. Если данные загружаются из файла, на экране появится диалог для редактирования учетной информации компьютера. При необходимости введите актуальную учетную информацию.

Сравнение паспортов

Если список паспортов защищаемого компьютера содержит несколько паспортов (например, проект паспорта, текущий утвержденный паспорт и ранее утвержденный паспорт), между этими паспортами можно выполнять сравнение имеющихся данных о СПС. Сравнение выполняется в программе управления в централизованном режиме работы. Правами для сравнения паспортов обладает пользователь с привилегией "Просмотр информации".

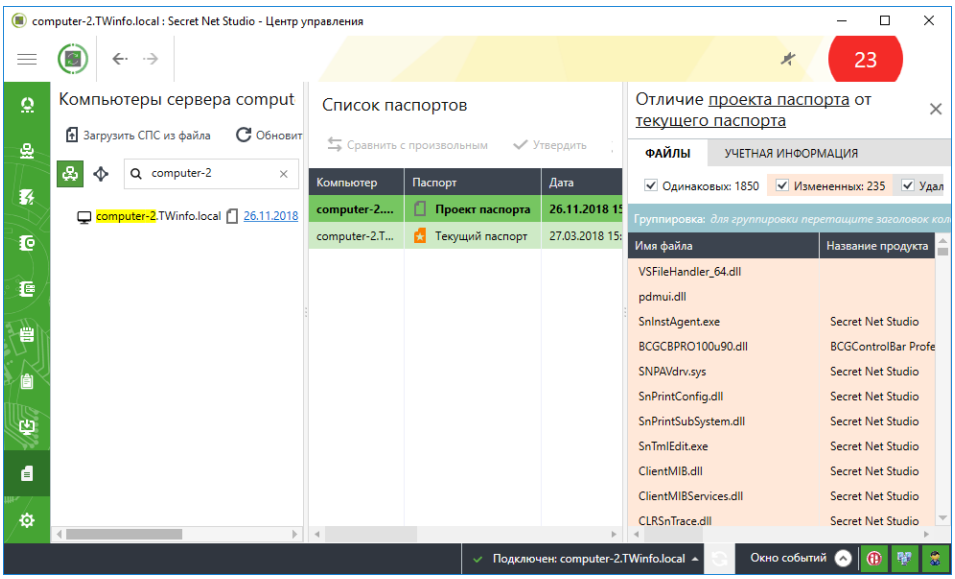
Для сравнения данных в паспортах:

1. В средней части панели "Паспорт ПО" выберите паспорта для сравнения. Если сравнение нужно выполнить между соседними паспортами в списке (например, между проектом паспорта и текущим утвержденным паспортом) — достаточно выделить только тот, который был получен позже (в приведенном примере — проект паспорта). Для сравнения любых двух паспортов в списке выделите их, удерживая нажатой клавишу <Ctrl>.



2. Вызовите контекстное меню выделенного паспорта и выберите соответствующую команду:
   - "Сравнить с предыдущим" — чтобы сравнить с предыдущим паспортом по списку;
   - "Сравнить с произвольным" — чтобы сравнить с другим выбранным паспортом.

   После загрузки данных в правой части панели "Паспорт ПО" появятся результаты сравнения.



На вкладке "Файлы" отображаются сведения о файлах. Общая сводная информация о результатах сравнения представлена в панели над списком. Панель содержит сведения о количестве обнаруженных файлов: одинаковых, измененных, удаленных и новых. По каждому набору файлов можно выполнить фильтрацию списка, чтобы отключить отображение ненужных элементов (например, одинаковых файлов). Для фильтрации удалите отметки рядом с названиями соответствующих кнопок в панели.

Примечание. В списке файлов используется цветовое оформление в зависимости от результатов сравнения. Каждый элемент выделен тем цветом, который соответствует кнопке в панели сводных результатов. Например, одинаковые файлы в сравниваемых паспортах отображаются на белом фоне.

3. Для упорядочивания списка файлов используйте средства группировки и сортировки сведений:
   - в режиме группировки применяется комбинированный вид отображения таблицы и иерархического списка с возможностью сворачивания групп элементов. Настройка осуществляется в области "Группировка". Чтобы разбить элементы по группам с одинаковыми значениями колонок (например, по названиям продуктов и по версиям), последовательно переместите заголовки этих колонок в область группировки. Внутри области можно перемещать заголовки относительно друг друга и переключать режим сортировки;
   - сортировка колонок выполняется стандартными способами. Чтобы отсортировать таблицу по значениям колонки, нажмите на ее заголовок. Для сортировки в обратном направлении нажмите заголовок еще раз.
4. При необходимости настройте состав колонок и порядок их следования в таблице. Для этого вызовите контекстное меню в строке заголовков колонок, выберите команду "Настройка колонок" и настройте параметры отображения в появившемся диалоге.
5. Перейдите на вкладку "Учетная информация".

Вкладка содержит список параметров учетной информации компьютера. Для параметров в отдельных колонках указаны значения, сохраненные в сравниваемых паспортах.

6. После завершения анализа данных можно очистить панель сведений с помощью кнопки закрытия в правом верхнем углу.

Проверка действительности подписи для утвержденных паспортов

Для защиты от подмены утвержденного паспорта предусмотрена процедура проверки подписи. Процедура выполняется в программе управления в централизованном режиме работы. Правами для проверки обладает пользователь с привилегией "Просмотр информации".

Для проверки подписи паспорта:

1. Загрузите криптографические ключи с вашего ключевого носителя. Загрузка ключей может выполняться автоматически при входе в систему с использованием персонального идентификатора или с помощью специальной команды "Ключи пользователя | Загрузить" в контекстном меню пиктограммы Secret Net Studio.

   Примечание. Дополнительные сведения о загрузке и выгрузке криптографических ключей см. в документе [3].

2. В программе управления откройте панель "Паспорт ПО" и в левой части выберите нужный компьютер. При необходимости для быстрого перехода к компьютеру используйте средства фильтрации и поиска, расположенные над списком объектов.
3. В средней части панели "Паспорт ПО" вызовите контекстное меню утвержденного паспорта и выберите команду "Проверить подпись".

   Программа выполнит проверку действительности подписи, после чего будет выведен результат в колонке "Проверка подписи".

Утверждение проекта паспорта

Утверждение проекта паспорта в качестве текущего паспорта компьютера выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает пользователь с привилегией "Утверждение паспорта ПО".

Для утверждения проекта паспорта:

1. Загрузите криптографические ключи с вашего ключевого носителя. Загрузка ключей может выполняться автоматически при входе в систему с использованием персонального идентификатора или с помощью специальной команды "Ключи пользователя | Загрузить" в контекстном меню пиктограммы Secret Net Studio.

   Примечание. Дополнительные сведения о загрузке и выгрузке криптографических ключей см. в документе [3].

2. В программе управления откройте панель "Паспорт ПО" и в левой части выберите нужный компьютер. При необходимости для быстрого перехода к компьютеру используйте средства фильтрации и поиска, расположенные над списком объектов.
3. В средней части панели "Паспорт ПО" вызовите контекстное меню проекта паспорта и выберите команду "Утвердить".

   На экране появится запрос на подтверждение выполнения операции.

4. Нажмите кнопку "Утвердить" в диалоге запроса.

   После завершения операции проект паспорта станет текущим паспортом компьютера, а предыдущий останется в списке в качестве одного из ранее утвержденных паспортов.

Резервное копирование паспортов

Для хранения и загрузки паспортов на сервере безопасности создается специальная файловая структура — хранилище паспортов ПО. Хранилище размещается в каталоге установки сервера безопасности, подкаталог \Passport. При необходимости создания резервной копии паспортов скопируйте содержимое подкаталога \Passport на предназначенный для этого ресурс.

Удаление неактуальных паспортов

В списке паспортов защищаемого компьютера можно удалять неактуальные паспорта, кроме текущего утвержденного паспорта. При этом если не было выполнено резервное копирование хранилища паспортов, восстановить удаленный паспорт будет невозможно.

Удаление паспортов из списка выполняется в программе управления в централизованном режиме работы. Правами для выполнения операции обладает пользователь с привилегией "Удаление паспорта ПО".

Для удаления одного или нескольких паспортов компьютера:

1. В средней части панели "Паспорт ПО" выберите паспорта для удаления.
2. Вызовите контекстное меню одного из выделенных паспортов, выберите команду "Удалить" и подтвердите удаление в появившемся диалоге запроса.

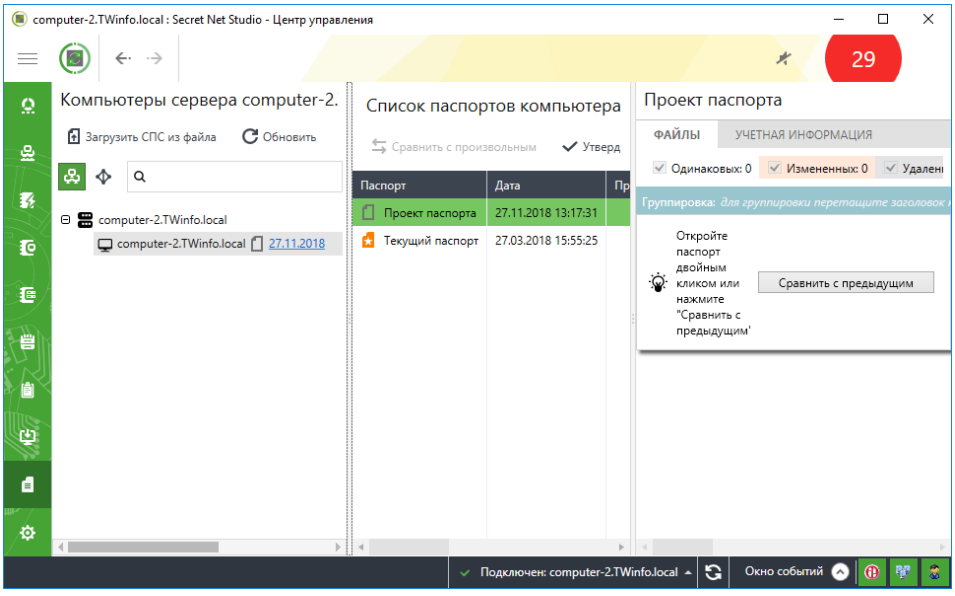
Восстановление паспортов из резервной копии

Хранилище паспортов ПО на сервере безопасности можно дополнять из резервной копии. После этого можно снова загрузить в программу управления те паспорта, которые были удалены как неактуальные.

Процедура восстановления паспортов выполняется на сервере безопасности и в программе управления в централизованном режиме работы. Правами для выполнения операции в программе управления обладает пользователь с привилегией "Синхронизация базы данных паспортов ПО".

Для восстановления паспорта из резервной копии:

1. На компьютере сервера безопасности скопируйте файлы из резервной копии в подкаталог \Passport каталога установки сервера безопасности.
2. В программе управления откройте панель "Паспорт ПО" и в левой части выберите сервер безопасности. Для отображения серверов безопасности нужно включить кнопку "Структура ОУ" в панели средств фильтрации и поиска, расположенных над списком объектов.



3. Вызовите контекстное меню выбранного сервера и выберите команду "Синхронизировать БД паспортов ПО".

Экспорт паспортов

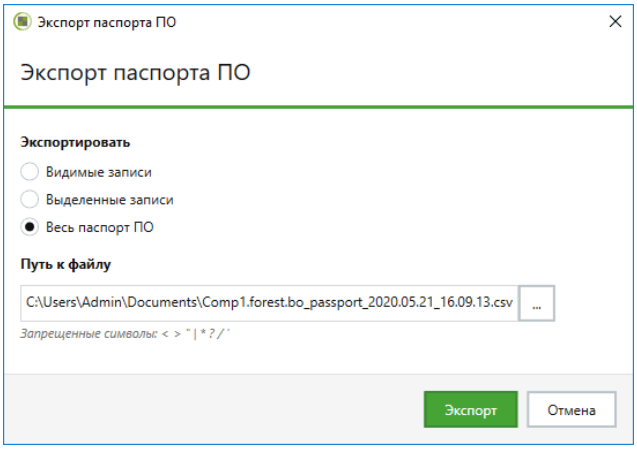
Имеется возможность экспорта паспорта ПО или отдельных записей о состоянии программной среды в файлы формата CSV.

Экспорт паспортов выполняется в программе управления в централизованном режиме работы.

Для экспорта паспорта:

1. В средней части панели "Паспорт ПО" вызовите контекстное меню паспорта, который требуется экспортировать, и выберите команду "Открыть".
2. При необходимости экспорта отдельных записей выполните фильтрацию по нужным параметрам или выберите в списке нужные записи. Для выбора нескольких записей нажмите и удерживайте клавишу <Ctrl>.
3. На вкладке "Файлы" нажмите кнопку "Экспорт".

   На экране появится мастер экспорта паспортов.



4. Выберите необходимый вариант экспорта:
   - "Видимые записи" — экспорт записей в соответствии с примененными фильтрами;
   - "Выделенные записи" — экспорт записей, выбранных в списке;
   - "Весь паспорт ПО" — экспорт всех записей выбранного паспорта.
5. Укажите полный путь для сохранения файла и нажмите кнопку "Экспорт".

Регистрируемые события в журнале сервера безопасности

Операции с паспортами, выполняемые в программе управления в централизованном режиме работы, протоколируются в журнале сервера безопасности. Предусмотрена регистрация следующих событий:

- утверждение паспорта ПО;
- ошибка утверждения паспорта ПО;
- удаление паспорта ПО;
- ошибка удаления паспорта ПО;
- загрузка проекта паспорта ПО;
- ошибка загрузки проекта паспорта ПО;
- синхронизация паспортов ПО;
- ошибка синхронизации паспортов ПО;
- запуск сбора данных СПС;
- сбор данных СПС завершен;
- ошибка в процессе сбора данных СПС;
- сохранение данных СПС.

Глава 8
Настройка контроля устройств

Общие сведения о разграничении доступа к устройствам

Для защиты доступа к устройствам компьютера используются механизм контроля подключения и изменения устройств и механизм разграничения доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля подключения и изменения устройств предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера, а также для поддержания в актуальном состоянии списка устройств компьютера. По списку устройств с помощью второго механизма выполняется разграничение доступа пользователей к устройствам. Часть функций разграничения доступа к устройствам реализуется с использованием механизма полномочного управления доступом.

Список устройств

Для представления множества устройств, установленных или подключаемых к защищаемым компьютерам, используется иерархическая схема списка устройств. Устройства группируются в классы, а классы, в свою очередь, включены в состав групп. Группы являются элементами объединения верхнего уровня. Количество групп фиксировано. Предусмотрены следующие группы:

- "Локальные устройства" — объединяет фиксированные устройства компьютера, для которых не предполагается ограничивать подключение (например, последовательные и параллельные порты, процессоры, оперативная память);
- "Устройства USB" — объединяет устройства, подключаемые к шине USB;
- "Устройства PCMCIA" — объединяет устройства, подключаемые к шине PCMCIA;
- "Устройства IEEE1394" — объединяет устройства, подключаемые к шине IEEE1394;
- "Устройства Secure Digital" — объединяет устройства, подключаемые к шине Secure Digital;
- "Сеть" — объединяет устройства, являющиеся сетевыми интерфейсами (адаптеры). Если сетевым интерфейсом является нефиксированное подключаемое устройство, такое устройство может также присутствовать и в другой группе. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве сетевого интерфейса.

Некоторые классы допускают дополнительное разбиение устройств по моделям. Модели объединяют устройства с одинаковыми идентификационными кодами, присвоенными производителем (VID и PID). В списке устройств присутствуют предопределенные модели — например, модели электронных идентификаторов. Также в список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды. В дальнейшем при обнаружении нового устройства с такими же идентификационными кодами это устройство автоматически будет добавлено в качестве экземпляра к той же модели. За счет этого можно управлять одинаковыми устройствами без необходимости настройки параметров каждого устройства по отдельности.

Для объектов каждого уровня (группа, класс, модель, устройство) определен набор параметров, с помощью которых настраиваются механизмы контроля подключения и изменения устройств, разграничения доступа к устройствам, теневого копирования и полномочного управления доступом. Иерархия списка устройств в большинстве случаев позволяет выполнять настройку как на уровне отдельного устройства, так и на уровне классов и групп.

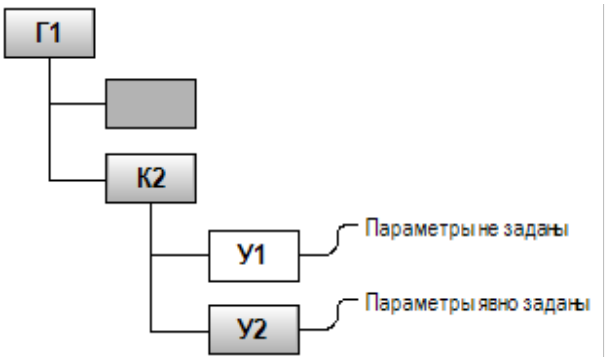
Полный список групп, классов и возможностей создания моделей устройств приведен в приложении на стр.**272**.

На компьютере список устройств создается сразу после установки клиентского ПО системы Secret Net Studio при первой загрузке ОС. Этот список устройств принимается как эталонная конфигурация компьютера. Он хранится в локальной базе данных системы Secret Net Studio и загружается в локальной политике.

Для централизованного управления устройствами на компьютерах с клиентом в сетевом режиме функционирования можно создать список устройств в групповой политике. После создания список устройств состоит из групп, классов и предопределенных моделей устройств. При необходимости в список можно добавить и конкретные устройства.

Правила наследования параметров в списке устройств

В рамках групповой или локальной политики права доступа к каждому объекту, а также параметры контроля устройств определяются в соответствии с правилами наследования или явного задания параметров. Параметры могут быть заданы для групп, классов, моделей или конкретных устройств. При задании параметров может использоваться принцип наследования параметров от вышестоящих элементов иерархии в списке. При этом явно заданные параметры имеют приоритет перед наследуемыми параметрами старших элементов иерархии. Например, если для устройства явно заданы особые параметры доступа, они будут применяться независимо от того, какие параметры заданы для класса и группы.



В приведенном на рисунке примере устройство "У1" наследует параметры, заданные для класса "К2". Для устройства "У2" действуют явно заданные параметры, которые могут отличаться от параметров, заданных для класса "К2".

Возможности управления

Управление устройствами осуществляется в Центре управления (централизованное управление) или в Локальном центре управления (локальное управление).

Предусмотрены следующие методы управления устройствами:

- управление с использованием только локальной политики каждого компьютера;
- управление с использованием групповых политик для элементов верхнего уровня (групп, классов и моделей устройств) и локальной политики каждого компьютера для конкретных устройств;
- управление с использованием групповых политик для всех элементов списка устройств.

Для компьютеров с установленным клиентом в автономном режиме функционирования недоступны возможности управления с использованием групповых политик.

Редактирование параметров групповых политик осуществляется на рабочем месте администратора безопасности в Центре управления. Параметры локальной политики можно настраивать как в Центре управления, так и в Локальном центре управления.

Управление с использованием групповых политик для элементов верхнего уровня

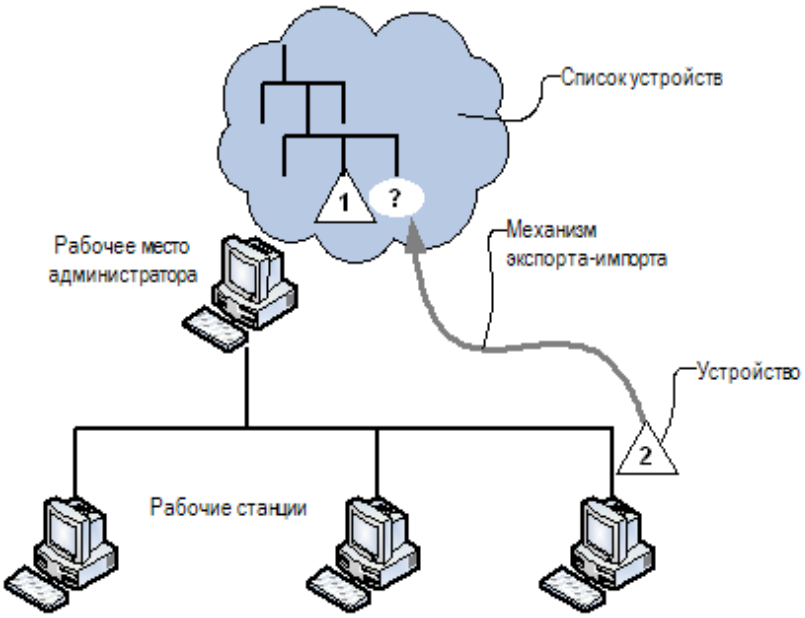
Данный вариант является предпочтительным, когда требуется обеспечить общие принципы контроля устройств на защищаемых компьютерах и нет необходимости централизованной настройки для отдельных устройств. Администратору безопасности достаточно настроить параметры использования для групп, классов и моделей устройств в нужных групповых политиках — например, в политике организационного подразделения. Параметры групповой политики будут применяться на компьютерах независимо от того, какие параметры заданы для этих элементов в локальной политике каждого компьютера. При этом настройка параметров использования конкретных устройств выполняется в локальной политике каждого компьютера.

Управление с использованием групповых политик для всех элементов списка устройств

Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных устройств, можно выполнить их настройку в политике домена, организационного подразделения или сервера безопасности.

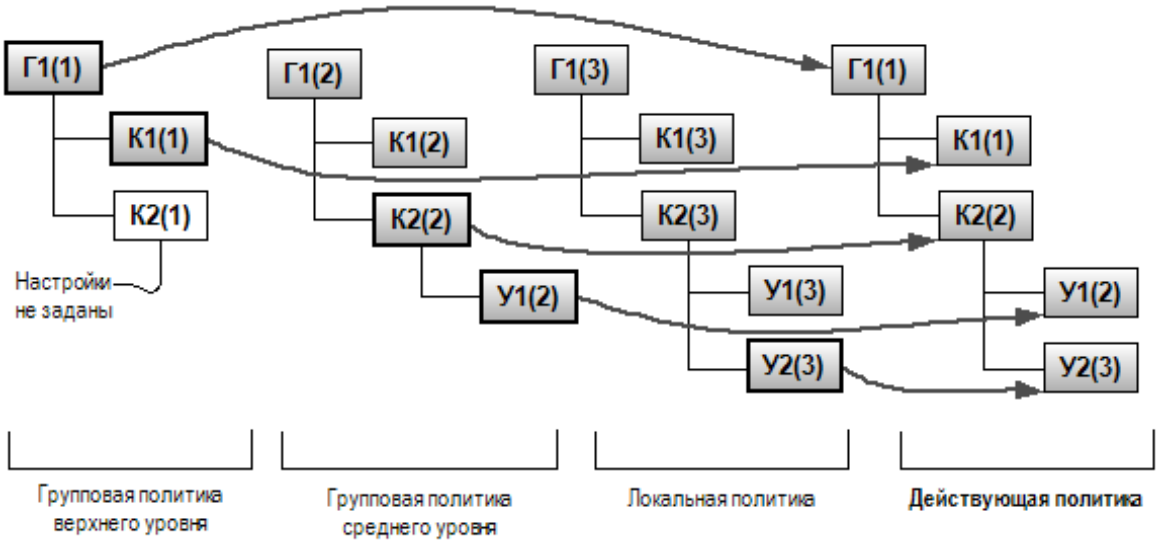
Устройства, параметры которых нужно настроить, должны быть добавлены в список групповой политики. В список устройств политики можно добавить сведения об устройствах, подключенных к какому-либо компьютеру с установленным клиентским ПО системы Secret Net Studio.

Описание предусмотренных возможностей для добавления устройств см. на стр.**87**.



Особенности применения групповых политик со списками устройств

При входе пользователя в систему значения параметров контроля и доступа к устройствам устанавливаются в соответствии с действующей политикой. Действующая политика определяется при применении заданных параметров групповых политик с учетом их приоритета. Наименьший приоритет имеют параметры локальной политики. Они могут действовать только в случае отсутствия таких параметров в групповых политиках других уровней (в политиках доменов, организационных подразделений и серверов безопасности). Наивысший приоритет имеет групповая политика корневого сервера безопасности. Частный пример применения параметров групповых политик для групп (Г), классов (К) и отдельных устройств (У) представлен на рисунке:



Начальные параметры использования устройств

После установки Secret Net Studio в локальной политике заданы следующие правила использования устройств, которые распространяются на всех пользователей компьютера:

- Для групп "Локальные устройства" и "Сеть" включен режим контроля "Устройство постоянно подключено к компьютеру". Для остальных групп включен режим "Подключение устройства разрешено".
- Для всех обнаруженных жестких дисков, а также сменных и оптических включен режим контроля "Устройство постоянно подключено к компьютеру" с дополнительным параметром "Блокировать компьютер при изменении устройства". При этом для классов, к которым относятся такие устройства, включен режим "Подключение устройства разрешено".
- Для устройств с возможностью разграничения доступа предоставлен полный доступ трем стандартным группам пользователей: "Система", "Администраторы" и "Все".
- Теневое копирование отключено для всех устройств.
- Для устройств с возможностью назначения категории конфиденциальности включен режим доступа "Устройство доступно без учета категории конфиденциальности".
- Для сетевых интерфейсов разрешено функционирование независимо от уровней конфиденциальности сессий в режиме контроля потоков механизма полномочного управления доступом.
- Регистрируются все события категорий "Контроль аппаратной конфигурации" и "Разграничение доступа к устройствам".

- Разрешается использование локальных устройств и ресурсов в терминальных сессиях.

Общий порядок настройки для использования только разрешенных устройств

Настройка устройств, подключаемых к компьютеру, выполняется непосредственно на защищаемом компьютере средствами локального управления.

Внимание! Перед выполнением настройки устройств необходимо убедиться в том, что включена регистрация событий "Подключение устройства" и "Запрет подключения устройства" в разделе "Регистрация событий" для группы параметров "Контроль устройств". Анализ этих событий позволяет выявить составные устройства (см. стр.**85**). По умолчанию после установки системы защиты регистрация этих событий включена.

Чтобы обеспечить подключение и использование на компьютере только разрешенных устройств, выполните настройку последовательно и по отдельности для каждого такого устройства в следующем порядке:

1. Подключите к компьютеру устройство, которое будет использоваться.

   Устройство регистрируется в системе и ему назначаются права доступа и параметры контроля от вышестоящих объектов (моделей, классов, групп), к которым оно было отнесено.

2. Проведите анализ записей журнала, чтобы определить, является ли данное устройство составным.

   Для этого в Локальном центре управления перейдите к работе с журналами и откройте журнал Secret Net Studio с параметрами фильтрации записей по категории "Разграничение доступа к устройствам" и интервалу времени, соответствующему моменту подключения устройства.

   Если устройство является составным, в полученной выборке записей будут присутствовать несколько записей о событиях "Подключение устройства" или "Запрет подключения устройства". Для такого устройства сохраните сведения о вариантах его регистрации в системе. Названия устройств и их принадлежность к классам и группам указаны в событиях журнала.

3. Настройте параметры использования устройства:
   - политика контроля (см. стр.**94**);
   - разграничение доступа пользователей (см. стр.**95**);
   - теневое копирование (см. стр.**47**);
   - полномочное разграничение доступа (см. стр.**164** и стр.**168**).

   Пояснение. Для составного устройства необходимо выполнять настройку всех вариантов его представления в списке устройств в соответствии с рекомендациями, представленными ниже в параграфе "Особенности работы с составными устройствами".

4. Чтобы ограничить использование устройств в терминальных подключениях, включите запрет перенаправления (см. стр.**37**).
5. Отключите наследование параметров конкретных устройств от вышестоящих элементов списка и отключите разрешающие права для соответствующих моделей, классов и групп (см. стр.**94**). Например, разрешающие права можно отключить для группы "Устройства Secure Digital".
6. Повторите действия **1**–**5** для всех нужных устройств.

В результате пользователь сможет подключать и использовать только разрешенные устройства, а другие устройства будут запрещены. В дальнейшем можно удаленно разрешать использование новых устройств с помощью программы управления. Для этого по запросу пользователя администратор безопасности предлагает подключить нужное устройство (например USB-флеш-накопитель) к компьютеру на рабочем месте пользователя. После подключения устройства, даже если оно будет запрещено к использованию, сведения о нем появятся в списке устройств локальной политики. Администратор на своем рабочем месте в программе управления загружает параметры локальной политики соответствующего компьютера и выполняет необходимые действия для разрешения использования устройства.

Примечание. Отдельные инструкции для настройки использования подключаемых съемных дисков приведены в приложении на стр.274.

Особенности работы с составными устройствами

Некоторые устройства при подключении могут определяться системой как несколько устройств (далее — составные устройства). Для корректной настройки составного устройства необходимо выполнить однотипную настройку параметров для всех вариантов его представления в списке устройств.

Пояснение. Такие устройства выявляются в результате анализа записей журнала Secret Net Studio о событиях "Подключение устройства" и "Запрет подключения устройства" категории "Разграничение доступа к устройствам", зарегистрированных в момент подключения устройства к компьютеру.

Для примера рассмотрим работу с картами памяти MMC/SD. Большинство таких карт определяются как устройства группы "Устройства Secure Digital". В этом случае для разграничения доступа к SD-картам параметры контроля устройств, права доступа и параметры теневого копирования должны задаваться через группу устройств "Устройства Secure Digital", класс "Карточки памяти" или через конкретный экземпляр устройства, к которому необходимо разграничить доступ.

На некоторых моделях компьютеров подключаемые карты памяти MMC/SD определяются еще и как сменные диски и появляются в двух местах списка устройств: в классе "Сменные диски" группы "Локальные устройства" и в группе "Устройства Secure Digital". Это связано с особенностями реализации контроллеров на таких компьютерах. При этом подсистемы контроля аппаратной конфигурации и разграничения доступа к устройствам корректно обрабатывают данные устройства. Но в этом случае необходимо назначать одинаковые правила работы (параметры контроля устройств, права доступа, параметры теневого копирования) для каждого из двух устройств, добавленных в список.

При подключении SD-карт через устройство USB Card Reader подключаемые карты памяти MMC/SD могут не появляться в списке устройств как устройства группы "Secure Digital", а определяться только как подключенное устройство USB Card Reader в классе "Устройства хранения" группы "Устройства USB". Для разграничения доступа к SD-картам в таком случае параметры контроля устройств, права доступа и параметры теневого копирования должны задаваться через устройство USB Card Reader в классе "Устройства хранения" группы "Устройства USB".

Управление списком устройств

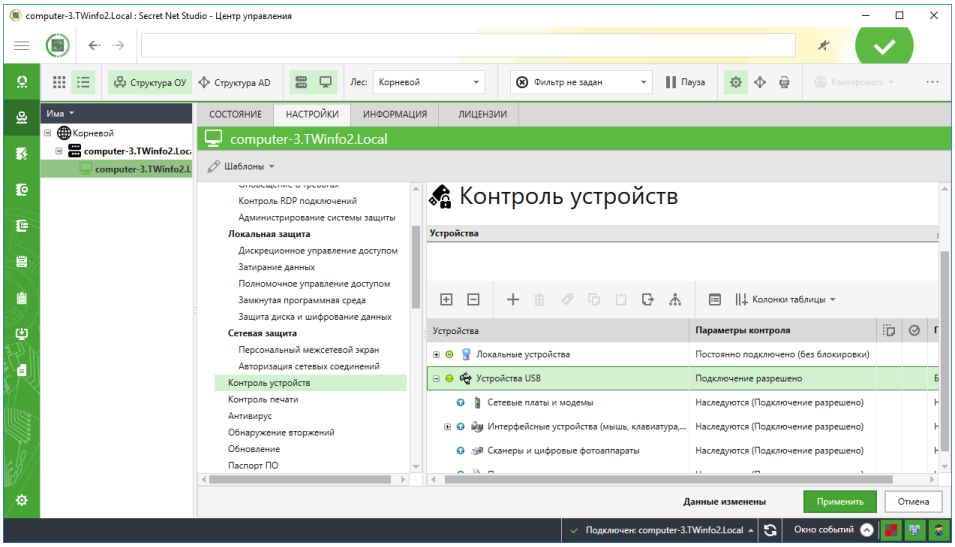
Загрузка списка устройств

Ниже приводится описание процедуры загрузки списка устройств при работе с Центром управления. Загрузка списка устройств локально выполняется аналогично с использованием Локального центра управления.

Для загрузки списка устройств:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Устройства".

   Пример списка представлен на следующем рисунке.



В локальной политике в список устройств автоматически добавляются все обнаруженные устройства компьютера. Также в этот список помещаются сведения об устройствах, подключенных на терминальных клиентах данного компьютера во время терминальных сессий (при условии, что эти устройства разрешены для использования). Подключенные в данный момент устройства отображаются в нормальном виде, отключенные — с зачеркнутыми именами.

Элементы списка устройств имеют определенную конфигурацию параметров, обеспечивающую функционирование всех нужных устройств с учетом логики управления в системе Secret Net Studio. Конфигурация параметров не является одинаковой для различных элементов списка и зависит от принадлежности устройств группам, классам и от специфики использования устройств. Для удобного просмотра списка устройств и оперативного получения основных сведений о текущей конфигурации параметров предусмотрены специальные пиктограммы статуса, перечисленные в таблице ниже.

Пиктограмма	Описание
	Параметры контроля для устройства наследуются от вышестоящего элемента списка устройств
(серый цвет)	Режим контроля для устройства отключен
	Для устройства включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру
(зеленый цвет)	Для устройства включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать
(красный цвет)	Для устройства включен режим контроля, при котором устройство запрещается подключать к компьютеру

Основные команды управления

Основные команды для работы со списком устройств и альтернативные способы их выполнения приведены в таблице ниже. Другие возможные команды указаны в инструкциях данной главы.

Команда	Кнопка	Управляющие клавиши	Вызов из контекстного меню
Добавить устройство		<Ctrl>+<N>	Да
Удалить устройство		<Del>	Да
Добавить модель для устройства		<Ctrl>+<M>	Да
Сохранить (экспорт)		<Ctrl>+<S>	Да
Показать информацию об устройстве		—	Нет
Раскрыть список		<Стрелка вправо>	Нет
Свернуть список		<Стрелка влево>	Нет
Раскрыть все		—	Нет
Свернуть все		—	Нет

Создание списка устройств в групповой политике

При установке системы Secret Net Studio список устройств формируется отдельно для каждого компьютера в локальной политике. Для централизованного управления списками устройств могут использоваться групповые политики доменов, организационных подразделений и серверов безопасности.

По умолчанию в групповых политиках отсутствуют списки устройств. Поэтому для реализации централизованного управления необходимо создать список устройств в нужной групповой политике. Настройка групповых политик осуществляется в Центре управления.

Добавление и удаление элементов списка устройств

В списке устройств групповой политики можно добавлять сведения о конкретных устройствах. Это позволяет задать параметры для устройства централизованно или локально, если устройство ранее не подключалось к компьютеру или по каким-либо причинам отсутствует в списке.

В данном разделе приведены следующие инструкции:

- добавление моделей на основе устройства (см. ниже);
- добавление устройств с помощью мастера импорта устройств (см. стр.**88**), в том числе:
  - добавление устройств по идентификаторам (см. стр.**89**);
  - добавление устройств из csv-файла и создание такого файла вручную (см. стр.**91**);
  - экспорт сведений об устройствах из списка устройств (см. стр.**93**);
- добавление устройств методом вставки из буфера обмена (см. стр.**94**);
- удаление моделей (стр.**94**);

- удаление устройств из списка (см. стр.94).

Внимание! При добавлении устройства копируются заданные для него параметры контроля и доступа. Однако в некоторых случаях параметрам могут быть присвоены значения по умолчанию, если получение прежних значений технически невозможно. После добавления устройства обязательно проверьте заданные для него параметры и при необходимости откорректируйте их.

Добавление модели на основе устройства

Добавление модели позволяет управлять одинаковыми устройствами без необходимости настройки параметров каждого устройства по отдельности.

В список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды (VID и PID).

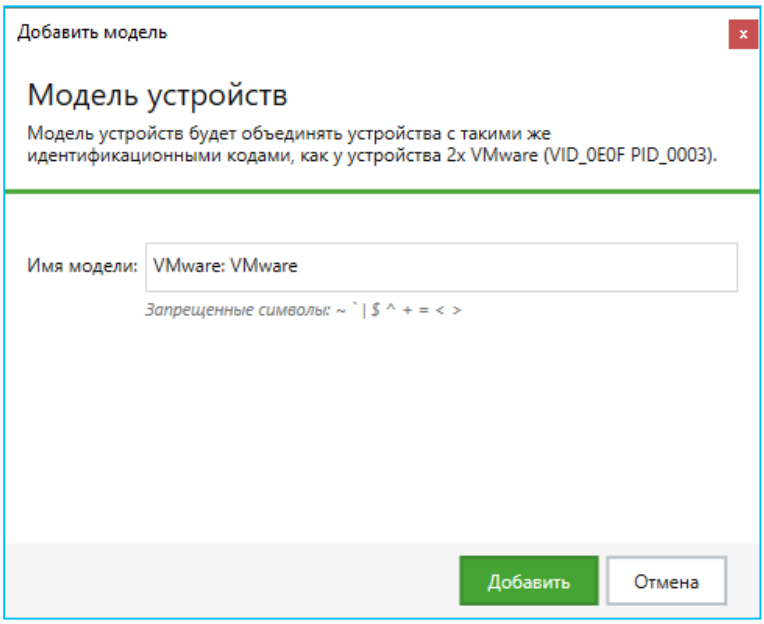
При добавлении модели для нее наследуются все настройки с вышестоящего объекта — класса устройств. Впоследствии можно изменить эти настройки.

Пояснение. Для некоторых классов устройств имеются предопределенные модели (см. стр.272).

Для добавления модели:

1. Выберите устройство с идентификационными кодами (VID и PID) и выберите команду "Добавить модель для устройства".

   На экране появится стартовый диалог мастера добавления модели.



2. Введите имя модели и нажмите кнопку "Добавить".

   В список устройств групповой политики добавится новая модель.

3. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Использование мастера импорта устройств

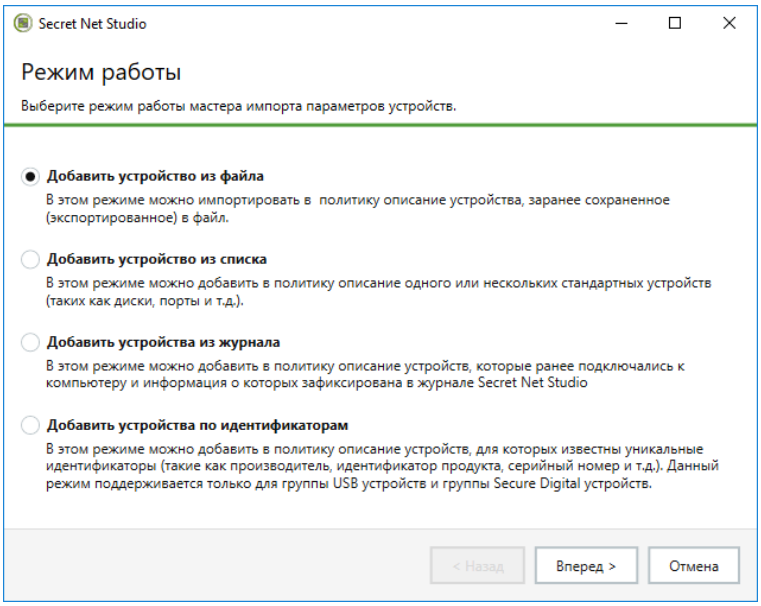
Мастер импорта предоставляет следующие возможности:

- импорт устройства из файла, в котором сохранены (экспортированы) сведения об устройстве;
- добавление стандартного устройства из предопределенного списка (например, порт ввода/вывода);
- добавление устройства, ранее зафиксированного в журнале Secret Net Studio – C;
- добавление устройства по параметрам.

Для импорта устройств в список групповой политики:

1. Выберите команду "Добавить устройство".

На экране появится стартовый диалог мастера импорта устройств.



2. Выберите вариант добавления устройства, нажмите кнопку "Вперед >" и следуйте инструкциям мастера.

Ниже приводится описание процедуры добавления устройств по идентификаторам.

Добавление устройств по идентификаторам

Режим добавления устройств по идентификаторам позволяет регистрировать устройства в политике контроля устройств. Такая возможность способствует:

- формированию списка устройств без их физического подключения к компьютеру;
- регистрации большого количества устройств одной модели одновременно.

Данный режим поддерживается только для групп устройств USB и SD.

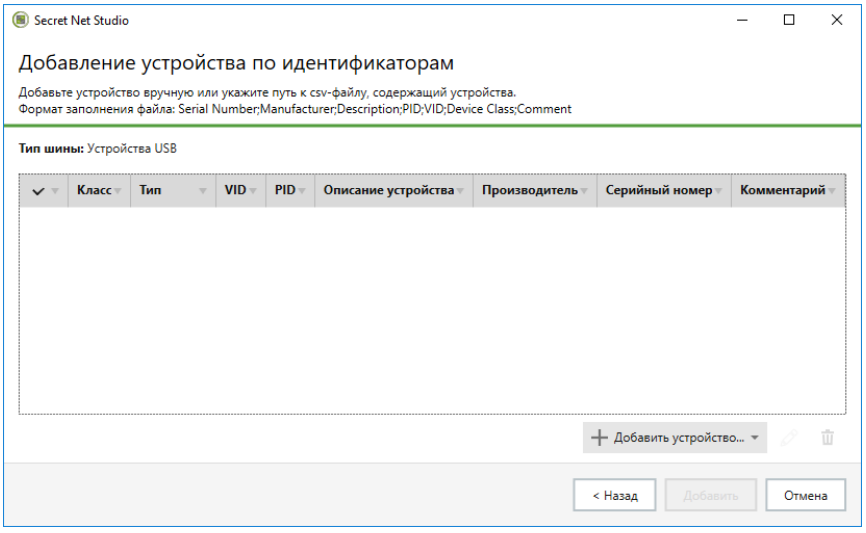
Для добавления устройств в список групповой политики:

1. Выберите группу устройств USB или SD либо объект из этих групп и выберите команду "Добавить устройство".

   На экране появится стартовый диалог мастера импорта устройств.

2. Выберите режим "Добавить устройства по идентификаторам" и нажмите кнопку "Вперед >".

   На экране появится диалог добавления устройств по идентификаторам.



Примечание. Параметр "Статус" может принимать следующие состояния:

- "Устройство готово к добавлению" – введены все параметры устройства, соответствующие контексту;
- "Устройство готово к добавлению, но не соответствует контексту" – введены все параметры устройства, но они не соответствуют контексту;
- "Устройство не готово к добавлению" – введены не все параметры устройства.

Сортировка колонки "Статус" выполняется стандартными способами. Чтобы отсортировать таблицу по состоянию колонки, нажмите на ее заголовок. Для сортировки в обратном направлении нажмите заголовок еще раз.

3. Сформируйте список устройств для импорта, добавив устройства вручную или из csv-файла (описание процедуры добавления устройств см. ниже).

   Все добавленные устройства помещаются в список, в котором можно отредактировать или удалить отдельно выбранное устройство, используя команды "Редактировать" или "Удалить".

4. Нажмите кнопку "Добавить".

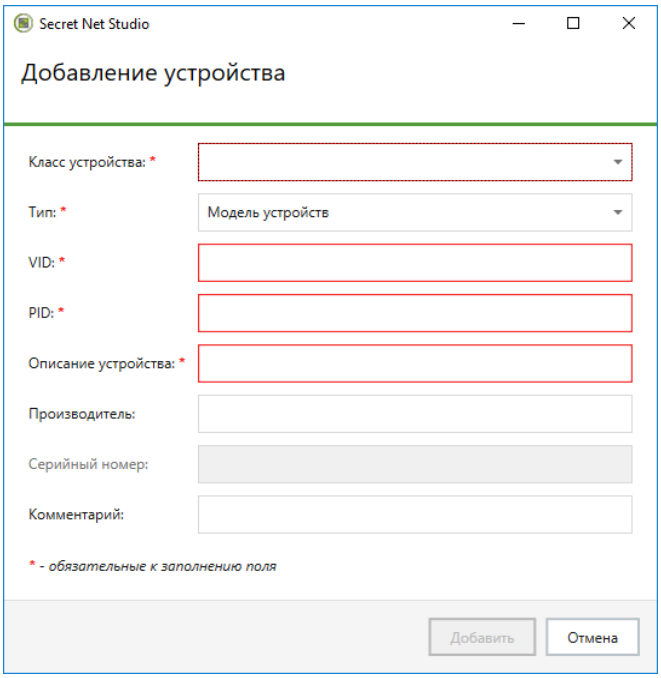
   В список устройств групповой политики добавятся новые объекты.

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Для добавления устройств вручную:

1. Выберите пункт "Добавить устройство вручную" (в этом случае процесс добавления нового устройства осуществляется с помощью ручного ввода его параметров).

   На экране появится диалог добавления устройства вручную.



Пояснение. Поля, выделенные красным цветом, являются обязательными для заполнения.

2. Заполните параметры устройства:

Параметр	Описание
Класс устройства	Содержит наименование класса устройства. Выберите нужный класс устройства из раскрывающегося списка. Для группы устройств SD предусмотрен класс устройства "Карточка памяти". Для группы устройств USB предусмотрен перечень классов устройств в соответствии с идентификатором (см. таблицу ниже)
Тип	Содержит наименование типа устройства. Выберите нужный тип устройства из раскрывающегося списка

Параметр	Описание
VID	Содержит идентификатор производителя устройства
PID	Содержит идентификатор модели устройства
Описание устройства	Содержит информацию об устройстве
Производитель	Содержит наименование компании, производящей устройство
Серийный номер	Содержит уникальный идентификационный номер устройства
Комментарий	Содержит дополнительные сведения об устройстве

Перечень идентификаторов классов устройств для группы устройств USB.

ID	Класс устройств
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

Примечание. Количество доступных для заполнения параметров зависит от класса добавляемого устройства.

3. Нажмите кнопку "Добавить".

   На экране появится диалог добавления устройства по идентификаторам.

Добавление устройств из файла

В этом случае процесс добавления новых устройств осуществляется с помощью ранее подготовленного csv-файла, который содержит параметры устройства. Ниже рассматривается процедура создания файла вручную.

Для добавления устройства из файла:

1. Выберите пункт "Добавить устройства из файла".

   На экране появится диалог для выбора csv-файла.

2. В поле "Имя файла" укажите csv-файл и нажмите кнопку "Открыть".

   В диалоге добавления устройств по идентификаторам появятся новые элементы списка, содержащие сведения о параметрах загруженных устройств. Для каждого добавленного устройства будет определено состояние параметра "Статус". Состояние "Устройство готово к добавлению" означает, что параметры были верно указаны в файле и устройство готово к добавлению в список групповой политики. Если параметр "Статус" принимает любое другое состояние, то это означает, что параметры были неверно указаны в файле и устройство не готово к добавлению в список групповой политики. Для исправления статуса устройства необходимо выбрать этот элемент из списка и отредактировать его параметры с помощью команды "Редактировать".

   Примечание. В случае если класс добавляемого устройства не соответствует классу объекта группы устройств, появится предупреждение. В диалоге добавления устройств по идентификаторам новый элемент списка не будет добавлен.

3. Нажмите кнопку "Добавить".

На экране появится диалог добавления устройства по идентификаторам.

Создание файлов с параметрами устройства

Файл с параметрами устройства позволяет полностью автоматизировать процесс добавления информации. Он создается в CSV-формате и является файлом представления, который содержит параметры подключаемого устройства. Файл создается вручную.

Совет. В качестве шаблона для заполнения параметров можно использовать файл, который находится на установочном диске \Tools\SecurityCode\SnDeviceAd\SnDeviceAd.csx. или использовать пример файла, приведенный ниже.

Для создания файла вручную:

- В текстовом редакторе создайте файл SnDeviceAD.csv, сформируйте его содержимое и сохраните файл.

Структура файла

Файл имеет следующую структуру:

Serial Number;Manufacturer;Description;PID;VID;Device Class;Comment
значение_ параметра_ 1;значение_ параметра_ 2;значение_ параметра_ 3;значение_параметра_4;значение_параметра_5;значение_параметра_6;значение_параметра_7
...
значение_ параметра_ A;значение_ параметра_ B;значение_ параметра_ C;значение_параметра_D;значение_параметра_E;значение_параметра_F;значение_параметра_G

Ниже представлен пример содержимого файла.

Serial Number;Manufacturer;Description;PID;VID;Device Class;Comment
;HP;HP LaserJet A4;0517;03f0;1007;Printer for print A4
1704HS03V1E8;Microsoft;Mouse;C077;046D;1003;Wired mouse
ZKY4VDHF;Transcend;USB;1000;8564;1008;USB for users

В приведенном примере предписывается:

Для первого устройства — принтер.

1. Серийный номер для принтера не указывается.
2. Производитель устройства "HP".
3. Описание устройства "HP LaserJet A4".
4. Идентификатор модели устройства "0517".
5. Идентификатор производителя устройства "03f0".
6. Класс устройства "Принтеры".
7. Комментарий "Printer for print A4".

Для второго устройства — компьютерная мышь.

1. Серийный номер "1704HS03V1E8".
2. Производитель "Microsoft".
3. Описание устройства "Mouse".
4. Идентификатор модели устройства "C077".
5. Идентификатор производителя устройства "046D".
6. Класс устройства "Интерфейсные устройства (мышь, клавиатура, ИБП и др.)".
7. Комментарий "Wired mouse".

Для третьего устройства — USB-флеш-накопитель.

1. Серийный номер "ZKY4VDHF".
2. Производитель "Transcend".
3. Описание устройства "USB".
4. Идентификатор модели устройства "1000".
5. Идентификатор производителя устройства "8564".
6. Класс устройства "Устройства хранения".
7. Комментарий "USB for users".

Экспорт сведений об устройствах из списка устройств

Сведения об устройствах, присутствующих в списке групповой политики, можно экспортировать в файлы. Экспорт осуществляется в файлы специального формата описания устройств системы Secret Net Studio (*.sndev). Содержимое файлов в дальнейшем можно импортировать с помощью мастера импорта (см. выше).

Примечание. Экспорт в файл формата *.sndev поддерживается только для устройств и моделей.

Для экспорта сведений:

1. Выберите команду "Сохранить".

   На экране появится стандартный диалог сохранения файла ОС Windows.
2. Укажите имя файла для сохранения сведений.

Использование буфера обмена для добавления устройств

Сведения об устройстве можно скопировать в буфер обмена из списка устройств другой политики. Методы использования буфера обмена для копирования и добавления устройств являются стандартными для ОС Windows.

Удаление модели

В отличие от класса, модель можно удалить из списка. При удалении модели содержащиеся в ней экземпляры устройства переходят в подчинение классу устройств.

Пояснение. Удаление всех экземпляров устройства не означает удаление модели устройств.

Для удаления модели:

1. Выберите модель в списке и нажмите кнопку "Удалить".
2. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Удаление устройств

Для удаления устройства из списка групповой политики выберите команду "Удалить".

Примечание. Для выбора нескольких устройств одного типа (на третьем уровне вложенности) нажмите и удерживайте клавишу <Ctrl>.

Контроль подключения и изменения устройств

Задание и настройка политики контроля устройств

Настройку политики контроля устройств можно выполнить:

- индивидуально для каждого устройства;
- для модели, класса или группы устройств с использованием принципа наследования параметров.

По умолчанию на компьютерах действуют параметры контроля устройств, заданные в локальной политике. Для компьютеров с установленным клиентом в сетевом режиме функционирования можно задать политику контроля устройств в групповых политиках (см. стр.**87**).

Для настройки политики контроля устройств:

1. Загрузите список устройств (см. стр.**85**).
2. Выберите строку с нужным элементом (группа, класс, модель, устройство).

   Примечание. Для выбора нескольких устройств одного типа (на третьем уровне вложенности) нажмите и удерживайте клавишу <Ctrl>.
3. При необходимости введите дополнительные сведения об элементе в ячейке колонки "Комментарий". Для этого нажмите кнопку в правой части ячейки.

   Примечание. По умолчанию колонка "Комментарий" не отображается. Для включения отображения нажмите кнопку "Колонки таблицы", которая расположена над списком устройств.

   Дополнительные сведения, указанные для устройства, сохраняются в журнале при регистрации событий, связанных с этим устройством.

4. Укажите нужные параметры в ячейке колонки "Параметры контроля". Для этого нажмите кнопку в правой части ячейки. Если для данного объекта требуется отключить наследование параметров от вышестоящего объекта и явно задать политику контроля, удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и настройте параметры контроля.

Поле "Устройство не контролируется"
Если в поле установлена отметка — для объекта отключен режим контроля
Поле "Устройство постоянно подключено к компьютеру"
Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру. В случае изменения состояния устройства в журнале регистрируется событие тревоги как попытка несанкционированного доступа, и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности. Для усиления защиты можно дополнительно включить режим автоматического блокирования компьютера при изменении состояния устройства. Для этого установите отметку в поле "Блокировать компьютер при изменении устройства". Разблокировать компьютер сможет только администратор безопасности
Поле "Подключение устройства разрешено"
Если в поле установлена отметка — для объекта 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 присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование
Поле "Подключение устройства запрещено"
Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. Попытки подключения устройства регистрируются в журнале как события тревоги. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Утверждение конфигурации

Изменения аппаратной конфигурации отслеживаются системой защиты для устройств с включенным режимом контроля "Устройство постоянно подключено к компьютеру". При обнаружении изменений в журнале регистрируются события тревоги. Если дополнительно включен режим "Блокировать компьютер при изменении устройства", выполняется блокировка компьютера. Снять блокировку компьютера и утвердить изменения в аппаратной конфигурации может только администратор.

Утверждение изменений аппаратной конфигурации выполняется в Центре управления. Описание процедуры см. в разделе "Утверждение изменений аппаратной конфигурации" документа [**1**].

Избирательное разграничение доступа к устройствам

При настройке разграничения доступа пользователей к устройствам выполняются действия:

1. Настройка прав доступа пользователей к устройствам (см. ниже).
2. Настройка регистрации событий и аудита операций с устройствами (см. стр.**97**).

Настройка прав доступа к устройствам

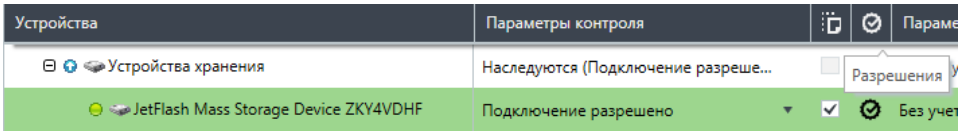
Права доступа пользователей могут устанавливаться для отдельных устройств или для классов.

Для настройки прав доступа к устройствам:

1. Загрузите список устройств (см. стр.**85**).
2. Выберите строку с нужным элементом списка (класс или устройство).

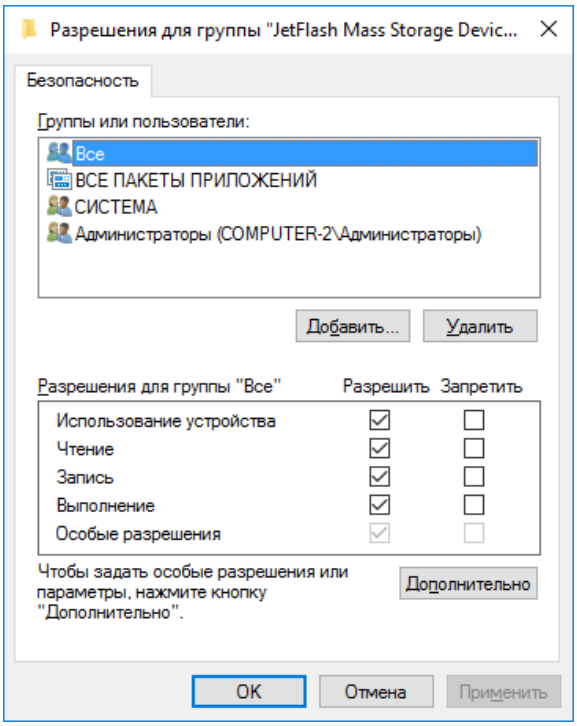
   Примечание. Для выбора нескольких устройств одного типа (на третьем уровне вложенности) нажмите и удерживайте клавишу <Ctrl>.

3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.



На экране появится диалог ОС Windows "Разрешения...".

Следует иметь в виду, что возможность вызова диалога "Разрешения..." предусмотрена только для тех устройств, для которых допускается настройка разрешений и запретов: порты, диски, носители данных (для системного диска управление разрешениями запрещено).



4. При необходимости отредактируйте список учетных записей в верхней части диалога.
5. Для изменения параметров доступа выберите в списке нужную учетную запись и затем расставьте разрешения и запреты на выполнение операций. При этом учитывайте принцип наследования параметров от родительских объектов дочерними: явно заданные параметры перекрывают унаследованные от родительских объектов.

   Для настройки особых разрешений нажмите кнопку "Дополнительно" и настройте параметры в открывшемся диалоговом окне.
6. После закрытия диалога "Разрешения..." нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка регистрации событий и аудита операций с устройствами

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, необходимо выполнить настройку регистрации событий. Настройка выполняется в Центре управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Контроль устройств". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр.**85**) — для этого используйте ссылку "Аудит" в правой части заголовка группы "Настройки" или группы "Устройства".

Настройка аудита успехов и отказов

Настройка аудита выполнения операций с устройствами может выполняться для классов и конкретных устройств.

Для настройки аудита:

1. Загрузите список устройств (см. стр.**85**).
2. Выберите строку с нужным элементом списка (класс или устройство).

   Примечание. Для выбора нескольких устройств одного типа (на третьем уровне вложенности) нажмите и удерживайте клавишу <Ctrl>.

3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.

   На экране появится диалог ОС Windows "Разрешения...".

4. Нажмите кнопку "Дополнительно".

   На экране появится диалоговое окно настройки дополнительных параметров.

5. Перейдите к диалогу "Аудит" и настройте параметры аудита ОС Windows.
6. После закрытия диалога "Разрешения..." нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Глава 9
Настройка контроля печати

Общие сведения о разграничении доступа к принтерам

Список принтеров

Настройка параметров использования принтеров осуществляется в отдельном списке "Принтеры". Параметры могут применяться по умолчанию при печати на любые принтеры или могут быть заданы для отдельных принтеров.

Печатающие устройства, представленные в списке принтеров, могут также присутствовать как устройства и в списке устройств. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве принтера.

На компьютере список принтеров создается сразу после установки клиентского ПО системы Secret Net Studio. Этот список представлен в локальной политике и хранится в локальной базе данных системы Secret Net Studio.

Для централизованного управления принтерами на компьютерах с клиентом в сетевом режиме функционирования можно создать список принтеров в групповой политике.

Возможности управления

Управление принтерами осуществляется в Центре управления (централизованное управление) или в Локальном центре управления (локальное управление).

Предусмотрены следующие методы управления принтерами:

- управление с использованием только локальной политики каждого компьютера;
- управление с использованием групповых политик для общих параметров по умолчанию и локальной политики каждого компьютера для конкретных принтеров;
- управление с использованием групповых политик для общих параметров по умолчанию и для конкретных принтеров.

Для компьютеров с установленным клиентом в автономном режиме функционирования недоступны возможности управления с использованием групповых политик.

Редактирование параметров групповых политик осуществляется на рабочем месте администратора безопасности в Центре управления. Параметры локальной политики можно настраивать в Центре управления и в Локальном центре управления.

Управление с использованием групповых политик для общих параметров по умолчанию

Данный вариант является предпочтительным, когда требуется обеспечить общие принципы контроля принтеров на защищаемых компьютерах и нет необходимости централизованной настройки для отдельных устройств. Администратору безопасности достаточно настроить параметры для элемента "Настройки по умолчанию" в нужных групповых политиках — например, в политике организационного подразделения. Параметры групповой политики будут применяться на компьютерах независимо от того, какие параметры заданы для этого элемента в локальной политике каждого компьютера. При этом настройка параметров использования конкретных принтеров выполняется в локальной политике каждого компьютера.

Управление с использованием групповых политик для общих параметров по умолчанию и для конкретных принтеров

Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных принтеров, можно выполнить их настройку в политике домена, организационного подразделения или сервера безопасности.

Для настройки параметров принтера его необходимо включить в список принтеров групповой политики. В список принтеров можно добавить любой доступный принтер.

Описание предусмотренных возможностей для добавления принтеров см. на стр.**100**.

Начальные параметры использования принтеров

После установки системы защиты в локальной политике по умолчанию заданы следующие правила использования принтеров, которые распространяются на всех пользователей компьютера:

- К принтерам предоставлен доступ стандартным группам пользователей: "Система", "Все" и "Все пакеты приложений".
- Теневое копирование отключено.
- Разрешается печать документов любой категории конфиденциальности.
- Разрешается использование локальных принтеров в терминальных сессиях.

Общий порядок настройки для печати только на разрешенных принтерах

Чтобы обеспечить возможность печати только на принтерах, разрешенных к использованию на компьютере, выполните настройку в следующем порядке:

1. После установки системы защиты откройте список принтеров операционной системы и проверьте наличие всех принтеров, которые планируется использовать. При отсутствии нужных принтеров выполните процедуры их установки (добавления в список ОС) в соответствии с рекомендациями производителя.

   Примечание. Необходимо учесть, что подключение к одним и тем же принтерам может выполняться различными способами. Например, если принтер (физическое устройство) установлен как локальный и как сетевой с IP-адресом. Для разграничения доступа к принтерам, подключение к которым будет осуществляться различными способами, необходимо выполнить процедуру установки принтера (добавления в список ОС) для каждого способа подключения. Этим будет обеспечена корректная идентификация таких принтеров системой защиты.

2. Добавьте принтеры в список групповой политики (см. стр.**100**).
3. Настройте параметры использования принтеров:
   - разграничение доступа пользователей (см. стр.**101**);
   - теневое копирование (см. стр.**47**);
   - полномочное разграничение доступа (см. стр.**165**).
4. Чтобы ограничить использование принтеров в терминальных подключениях, включите запрет перенаправления (см. стр.**37**).
5. В списке принтеров для элемента "Настройки по умолчанию" установите запрет печати для всех пользователей и включите ограничение печати документов всех категорий конфиденциальности.

В результате пользователь сможет отправлять документы на печать только на разрешенные устройства, а другие принтеры будут недоступны для использования. В дальнейшем при необходимости разрешить печать на новый принтер (или на тот же принтер, подключаемый другим способом) администратор может сам выполнить его установку, после чего добавить в список нужной политики и настроить параметры использования.

Управление списком принтеров

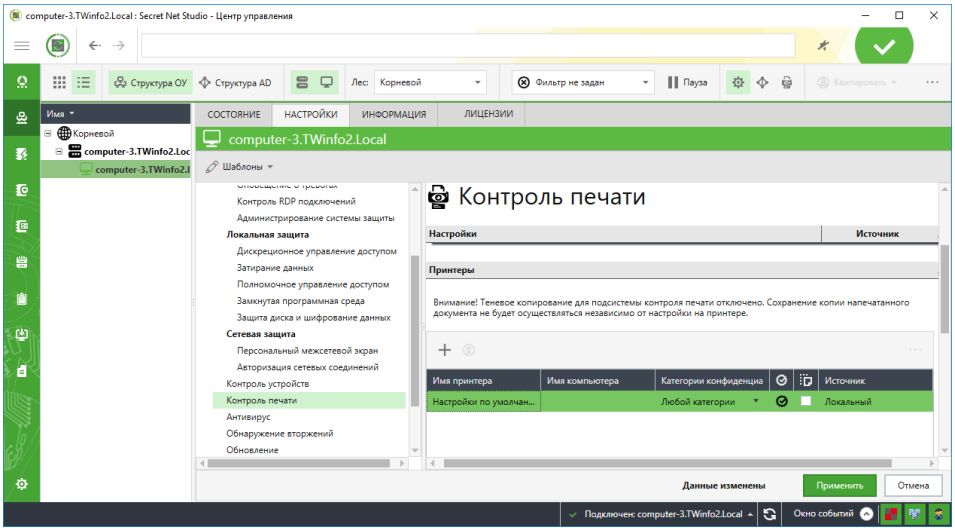
Загрузка списка принтеров

Ниже приводится описание процедуры загрузки списка принтеров при работе с Центром управления. Загрузка списка принтеров локально выполняется аналогично с использованием Локального центра управления.

Для загрузки списка принтеров:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Принтеры".

   Пример списка представлен на рисунке ниже.



Список принтеров изначально состоит из одного элемента "Настройки по умолчанию". Параметры использования принтеров, заданные для этого элемента, применяются ко всем принтерам, кроме тех, которые в явном виде присутствуют в списке принтеров. Добавление принтеров в список политики осуществляется с помощью специальной программы-мастера. Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента "Настройки по умолчанию".

Создание списка принтеров в групповой политике

Для централизованного управления параметрами принтеров могут использоваться групповые политики доменов, организационных подразделений и серверов безопасности.

По умолчанию в групповых политиках отсутствуют списки принтеров. Поэтому для реализации централизованного управления необходимо создать список принтеров в нужной групповой политике. Настройка групповых политик осуществляется в Центре управления.

Добавление и удаление элементов в списке принтеров

В список принтеров можно добавлять элементы, соответствующие конкретным принтерам. Добавление осуществляется с помощью специальной программы-мастера.

Использование мастера добавления принтеров

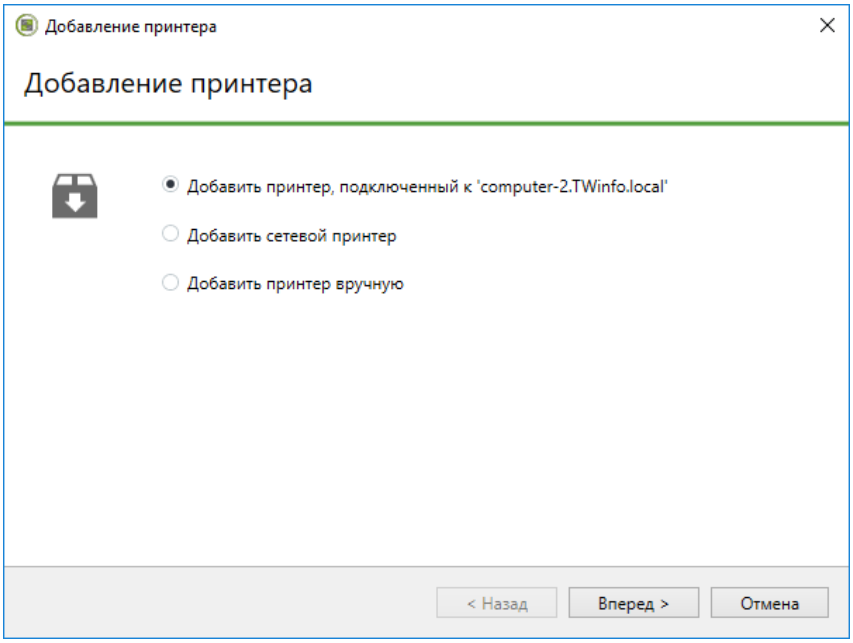
Мастер добавления предоставляет следующие возможности:

- добавление принтера, подключенного к выбранному компьютеру;
- добавление сетевого принтера;
- добавление принтера вручную.

Для добавления принтера в список групповой политики:

1. Вызовите контекстное меню любого элемента в списке принтеров и выберите команду "Добавить принтер".

   На экране появится стартовый диалог мастера добавления принтеров.



2. Выберите вариант добавления принтера, нажмите кнопку "Вперед >" и следуйте инструкциям мастера.

Удаление принтеров

При необходимости удалить принтер из списка групповой политики вызовите контекстное меню принтера и выберите команду "Удалить".

Избирательное разграничение доступа к принтерам

При настройке разграничения доступа к принтерам выполняются действия:

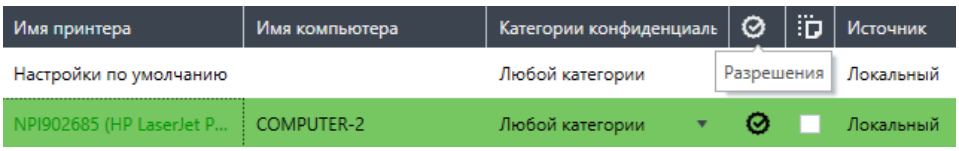
1. Настройка прав пользователей для печати на принтерах.
2. Настройка регистрации событий.

Настройка прав пользователей для печати на принтерах

Права пользователей для печати документов могут устанавливаться для конкретных принтеров или для элемента "Настройки по умолчанию".

Для настройки прав пользователей для печати:

1. Загрузите список принтеров (см. стр.**98**).
2. Выберите строку с нужным элементом списка.
3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.



На экране появится диалог ОС Windows "Разрешения...".

4. При необходимости отредактируйте список учетных записей в верхней части диалога.
5. Для изменения параметров доступа выберите в списке нужную учетную запись и затем отметьте разрешение или запрет на выполнение печати.

Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма контроля печати, необходимо выполнить настройку регистрации событий. Настройка выполняется в Центре управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Контроль печати". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр.**100**) — для этого используйте ссылку "Аудит" в правой части заголовка группы "Настройки" или группы "Принтеры".

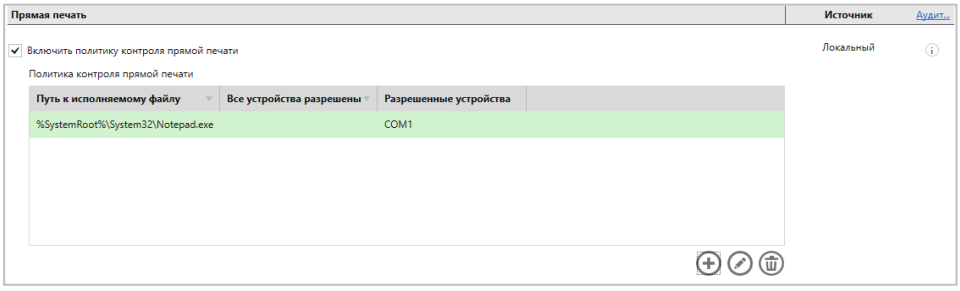
Прямой вывод на печать

Политики контроля прямого вывода на печать определяют процессы (приложения), которым разрешен прямой вывод на печать, минуя запрет на это действие.

Ниже приводится описание процедуры формирования списка политик контроля прямого вывода на печать.

Для управления политиками контроля прямого вывода на печать:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати | Прямая печать".
3. Для активации политики контроля прямого вывода на печать поставьте отметку в поле "Включить политику контроля прямой печати".

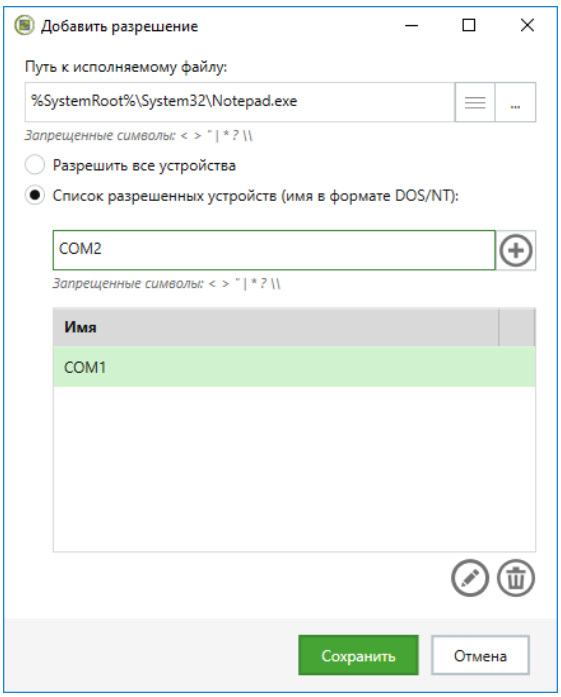


4. Сформируйте список политик контроля прямого вывода на печать. Управление списком политик осуществляется с помощью кнопок, расположенных под списком.

Кнопка	Описание
Добавить	Добавляет новую политику в список. Для новой политики выполняется настройка параметров в диалоговом окне (см. ниже)

Кнопка	Описание
Редактировать	Вызывает диалоговое окно для настройки параметров выбранной политики (см. ниже)
Удалить	Удаляет выбранный элемент из списка

При добавлении или редактировании политики на экране появится диалог для настройки параметров.



В диалоге укажите полный путь к исполняемому файлу. Для выбора пути к исполняемому файлу нажмите кнопку ... . При необходимости используйте переменные окружения из раскрывающегося списка, нажав кнопку . Настройте доступные параметры и нажмите кнопку "Сохранить".

Предусмотрены следующие варианты выбора разрешенных устройств:

- "Разрешить все устройства" — в этом случае для процесса будет разрешен доступ ко всем устройствам;
- "Список разрешенных устройств" — введите в поле наименование устройства в DOS- или NT-формате и нажмите кнопку справа . После добавления устройства оно появится в списке, который располагается ниже. Для изменения наименования устройства выберите его в списке и нажмите кнопку . Для удаления добавленного ранее устройства из списка нажмите кнопку .

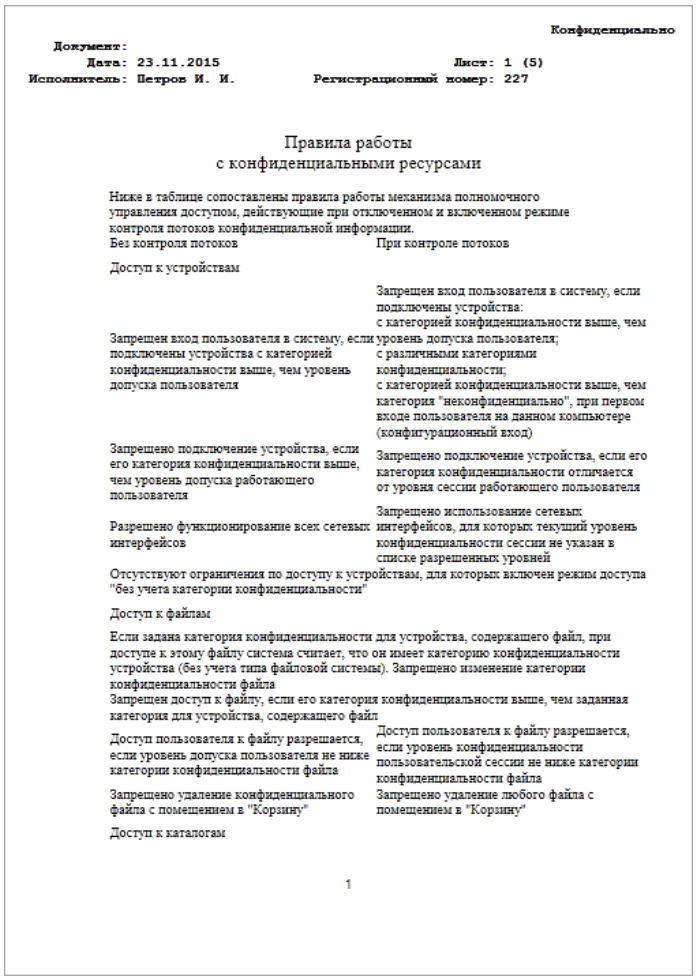
Примечание. Допускается указывать только локальный путь к исполняемому файлу, а не сетевой.

5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка маркировки распечатываемых документов

При включенном режиме маркировки в распечатываемые документы автоматически добавляются специальные маркеры (грифы), содержащие учетные сведения для печати. Маркер представляет собой особую форму со сведениями и обычно располагается в колонтитулах или на полях страниц. Сведения содержат информацию о распечатанном документе (например, когда распечатан, кем, сколько страниц). В системе маркер представлен как набор шаблонов, являющихся макетами определенных страниц документа: первой, последней, промежуточных и пр. В шаблонах заданы области расположения атрибутов со сведениями.

При печати документа происходит наложение макетов страниц из соответствующих шаблонов, и в результате на распечатанных листах вместе с содержимым документа выводятся сведения, относящиеся к маркеру. Печать этих сведений осуществляется независимо от расположения на листе текста самого документа. Пример распечатанной страницы с маркером в верхнем колонтитуле представлен на следующем рисунке.



Конфиденциально

Документ:
Дата: 23.11.2015 Лист: 1 (5)
Исполнитель: Петров И. И. Регистрационный номер: 227

Правила работы
с конфиденциальными ресурсами

Ниже в таблице сопоставлены правила работы механизма полномочного управления доступом, действующие при отключенном и включенном режиме контроля потоков конфиденциальной информации.

Без контроля потоков	При контроле потоков
Доступ к устройствам	
Запрещен вход пользователя в систему, если подключены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя	Запрещен вход пользователя в систему, если подключены устройства: с категорией конфиденциальности выше, чем уровень допуска пользователя; с различными категориями конфиденциальности; с категорией конфиденциальности выше, чем категория "неконфиденциально", при первом входе пользователя на данном компьютере (конфигурационный вход)
Запрещено подключение устройства, если его категория конфиденциальности выше, чем уровень допуска работающего пользователя	Запрещено подключение устройства, если его категория конфиденциальности отличается от уровня сессии работающего пользователя
Разрешено функционирование всех сетевых интерфейсов	Запрещено использование сетевых интерфейсов, для которых текущий уровень конфиденциальности сессии не указан в списке разрешенных уровней
Отсутствуют ограничения по доступу к устройствам, для которых включен режим доступа "без учета категории конфиденциальности"	
Доступ к файлам	
Если задана категория конфиденциальности для устройства, содержащего файл, при доступе к этому файлу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности файла	
Запрещен доступ к файлу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего файл	
Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла	Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла
Запрещено удаление конфиденциального файла с помещением в "Корзину"	Запрещено удаление любого файла с помещением в "Корзину"
Доступ к каталогам	

1

Маркеры могут применяться для печати документов любых категорий конфиденциальности, в том числе неконфиденциальных документов. При этом для одной категории допускается использовать несколько маркеров, чтобы пользователь мог самостоятельно выбирать нужный маркер из числа предусмотренных.

По умолчанию в системе задан набор маркеров с предопределенными шаблонами и атрибутами. При необходимости можно настроить маркировку в соответствии с действующими в организации требованиями оформления документов. Для настройки маркировки предоставляются возможности изменения параметров имеющихся объектов (маркеров, шаблонов, атрибутов, категорий конфиденциальности) и добавления новых объектов.

Управление режимом маркировки

Параметры, определяющие действие режима маркировки документов, представлены в списках объектов групповых политик.

Внимание! На компьютерах, входящих в один домен безопасности, должны применяться одинаковые параметры использования маркеров. Рекомендуется задать эти параметры в одной общей групповой политике.

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

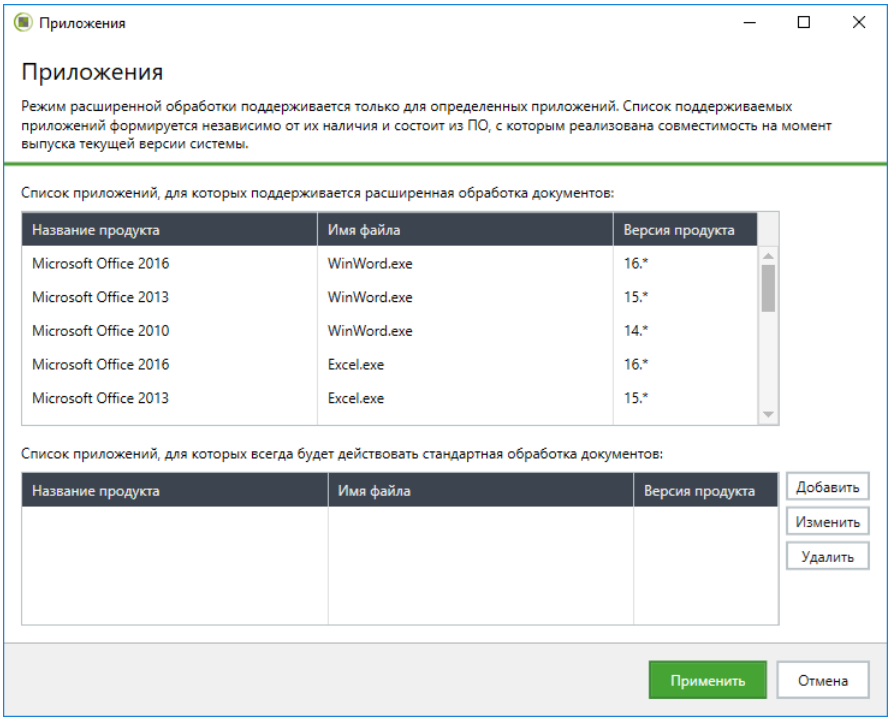
Для включения и настройки режима маркировки:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Настройки".
3. Для параметра "Маркировка документов" укажите нужное значение:
   - "Стандартная обработка" — режим может использоваться во всех поддерживаемых приложениях. В этом режиме предпочтительнее осуществлять печать документов целиком. При печати фрагмента документа маркер будет содержать сведения только о распечатанных страницах без учета общего количества страниц документа (так как распечатанный фрагмент воспринимается как отдельный документ). В журнале Secret Net Studio регистрируются события начала печати документа, окончания печати документа. При включенном теневом копировании в хранилище сохраняется копия распечатанного фрагмента, а не всего документа;
   - "Расширенная обработка" — режим может использоваться при печати из приложений, с которыми реализована совместимость (см. ниже). При отправке на печать происходит обработка всего документа независимо от объема распечатанного фрагмента. Поэтому при печати части документа подсчет и нумерация страниц осуществляются с учетом общего количества страниц документа. При этом в журнале Secret Net Studio регистрируются события начала печати документа, окончания печати документа, а также происходит регистрация начала и окончания печати каждой копии документа.

   Примечание. Если режим маркировки отключен, регистрация событий печати в журнале Secret Net Studio осуществляется в зависимости от состояния параметра групповой политики, который определяет действие функции теневого копирования для всех принтеров (см. раздел "Настройка теневого копирования" в документе []). Если для параметра "Теневое копирование" указано значение "Определяется настройками принтера", регистрируются события начала печати документа, окончания печати документа. При действующем значении "Отключено для всех принтеров" — в журнале регистрируются только события "Печать документа".
4. Настройте параметры использования маркеров. Для этого нажмите кнопку "Редактировать" и выполните настройку в появившемся окне программы редактирования маркеров (описание интерфейса и общий порядок действий при работе с программой приведены на стр.**108**). Если требуется вернуть параметры маркировки, заданные по умолчанию, — нажмите кнопку "По умолчанию".

5. Если включен режим "Стандартная обработка" — завершите процедуру, нажав кнопку "Применить" в нижней части вкладки "Настройки".
6. Если включен режим "Расширенная обработка" — проверьте список совместимых приложений и при необходимости укажите программы, в которых должен действовать стандартный режим обработки. Для этого выберите ссылку "Приложения, включенные в расширенную обработку".

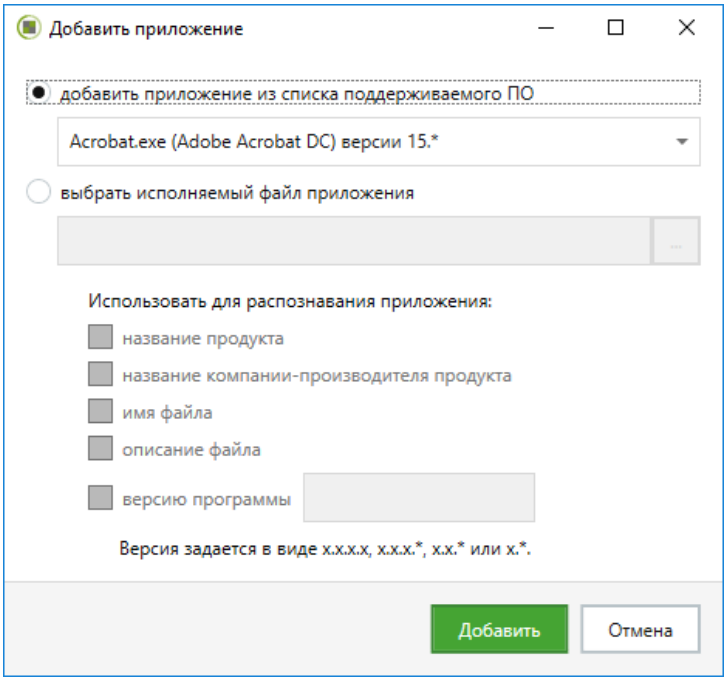
   На экране появится диалог со списками приложений.



7. Ознакомьтесь со списком совместимых приложений. Список формируется автоматически, независимо от наличия приложений на компьютере, и состоит из программ, с которыми реализована совместимость на момент выпуска текущей версии системы Secret Net Studio.
8. Отредактируйте, если требуется, список программ со стандартным режимом обработки и нажмите кнопку "Применить". Для редактирования списка используйте соответствующие кнопки справа:

Кнопка	Описание
Добавить	Вызывает диалог добавления приложения (см. ниже)
Изменить	Вызывает диалог настройки параметров распознавания выбранного приложения (см. ниже)
Удалить	Удаляет выбранное приложение из списка

При добавлении приложения на экране появляется диалог для выбора и настройки параметров распознавания приложения.

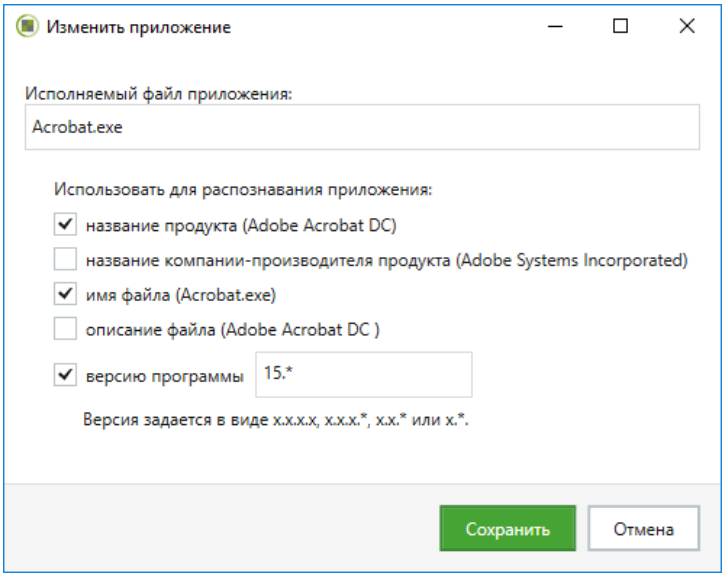


В диалоге выберите вариант добавления приложения, настройте доступные параметры и нажмите кнопку "Добавить". Предусмотрены следующие варианты выбора приложений:

- добавление из списка совместимых приложений — для этого установите отметку в поле "добавить приложение из списка поддерживаемого ПО" и выберите приложение из раскрывающегося списка (в этом случае параметры распознавания приложения системой будут заданы автоматически);
- добавление приложения по файлу его запуска — для этого установите отметку в поле "выбрать исполняемый файл приложения", нажмите кнопку справа и выберите файл в стандартном диалоге открытия файлов. При этом приложение должно быть установлено на данном компьютере, а исполняемый файл корректно указан. После выбора приложения настройте параметры его распознавания системой. Для этого отметьте подходящие методы, по которым система будет идентифицировать данное приложение (например, по производителю продукта, по имени файла и версии программы).

Примечание. Необходимо учитывать, что идентификация приложения будет выполняться по значениям, полученным для выбранных методов из указанного файла. В частности, название производителя продукта должно в точности совпадать с названием в файле. Поэтому, например, локализованные названия одного производителя (Microsoft и Майкрософт) будут восприниматься как различные.

При изменении выбранного приложения на экране появляется диалог для настройки параметров распознавания.



В диалоге отметьте методы, по которым система будет идентифицировать данное приложение, и нажмите кнопку "Изменить".

9. По окончании работы со списком приложений нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Для отключения режима маркировки:

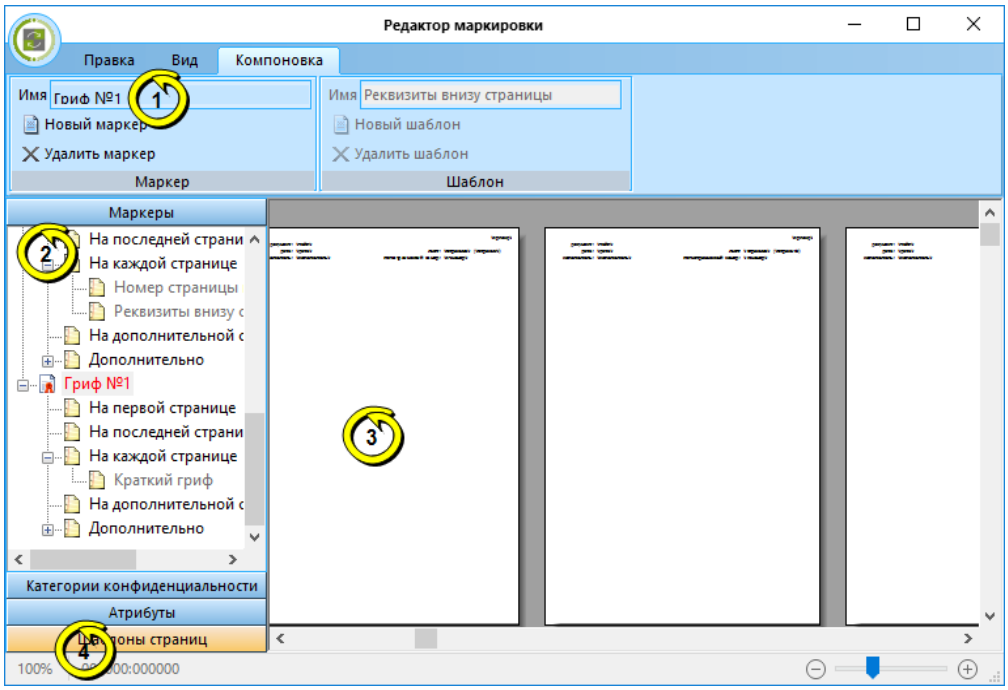
1. Выполните действия **1**–**2** вышеописанной процедуры.
2. Для параметра "Маркировка документов" укажите значение "Отключена".
3. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Программа редактирования маркеров

Программа редактирования маркеров предназначена для настройки маркировки документов, выводимых на печать. Запуск программы осуществляется в диалоге настройки параметра групповой политики "Маркировка документов" (см. стр.**105**).

Интерфейс программы

Пример окна программы редактирования маркеров представлен на рисунке:



Окно программы может содержать следующие элементы интерфейса.

1 — Лента

Содержит команды управления (инструменты) для выполнения действий в программе. Лента состоит из отдельных вкладок, в которых группируются команды в соответствии с их назначением. Для открытия вкладки используется ее заголовок.
Рабочее пространство в окне программы можно увеличить за счет переключения ленты в режим автоматического сворачивания. В этом режиме отображаются только заголовки вкладок, а разворачивание ленты происходит при выборе заголовка вкладки. Чтобы переключить режим отображения ленты, наведите указатель на заголовок любой вкладки и дважды нажмите левую кнопку мыши

2 — Панель выбора объектов

Содержит списки объектов и параметров использования объектов. Объекты и параметры группируются в следующих разделах:

- "Маркеры" — раздел предназначен для формирования списка маркеров (грифов). Для каждого маркера указываются шаблоны оформления определенных страниц при печати документа: первой страницы, последней, некоторых страниц, дополнительной или на обратной стороне листа. Маркер может содержать несколько шаблонов. При этом расположение данных указывается в шаблонах, но не в маркере. Формирование списка маркеров осуществляется с помощью команд группы "Маркер" на вкладке "Компоновка";
- "Категории конфиденциальности" — раздел предназначен для выбора маркеров, которые будут использоваться при печати документов определенных категорий конфиденциальности;
- "Атрибуты" — раздел предназначен для формирования списка атрибутов, которые будут использоваться в оформлении шаблонов страниц. Атрибуты представляют собой переменные, значения которых задаются перед отправкой документа на печать. Сведения для атрибута могут запрашиваться у пользователя или подставляются системой автоматически (например, текущая дата). Атрибуты с возможностью автоматического получения сведений обозначаются специальной пиктограммой. В списке можно добавлять и удалять атрибуты, для которых предусматривается запрос сведений у пользователя. Редактирование списка атрибутов осуществляется с помощью кнопок добавления и удаления элементов на панели инструментов в верхней части раздела "Атрибуты";
- "Шаблоны страниц" — раздел предназначен для формирования списка шаблонов оформления, которые указываются в маркерах для определенных страниц. Шаблон является макетом страницы, который накладывается на содержимое документа при его печати. Формирование списка шаблонов осуществляется с помощью команд группы "Шаблон" на вкладке "Компоновка".

Для перехода к нужному разделу используются соответствующие кнопки на панели выбора объектов

3 — Область редактирования

Предназначена для отображения и настройки параметров выбранного объекта. В зависимости от типа выбранного объекта область редактирования содержит:

- при выборе маркера — в области представлен общий вид маркировки всех страниц при печати документов с использованием маркера;
- при выборе элемента маркера, соответствующего определенным страницам, — область делится на две части: слева показан список шаблонов для выбора, справа — общий вид маркировки страницы при оформлении выбранными шаблонами;
- при выборе атрибута — область редактирования содержит поля с параметрами атрибута: внутреннее и отображаемое имя атрибута, описание и сведения о применении атрибута;
- при выборе шаблона — область редактирования содержит макет страницы для настройки оформления. Настройка выполняется посредством размещения элементов оформления (текста, рамок, значений атрибутов) внутри прямоугольных областей, аналогичных надписям в текстовых редакторах. Управление масштабом и общими параметрами отображения области редактирования осуществляется с помощью команд на вкладке "Вид". Управление элементами оформления и надписями — с помощью команд на вкладке "Правка". Чтобы отредактировать текст в надписи, наведите на нее указатель и дважды нажмите левую кнопку мыши — на экране появится диалог для ввода текста и вставки атрибутов

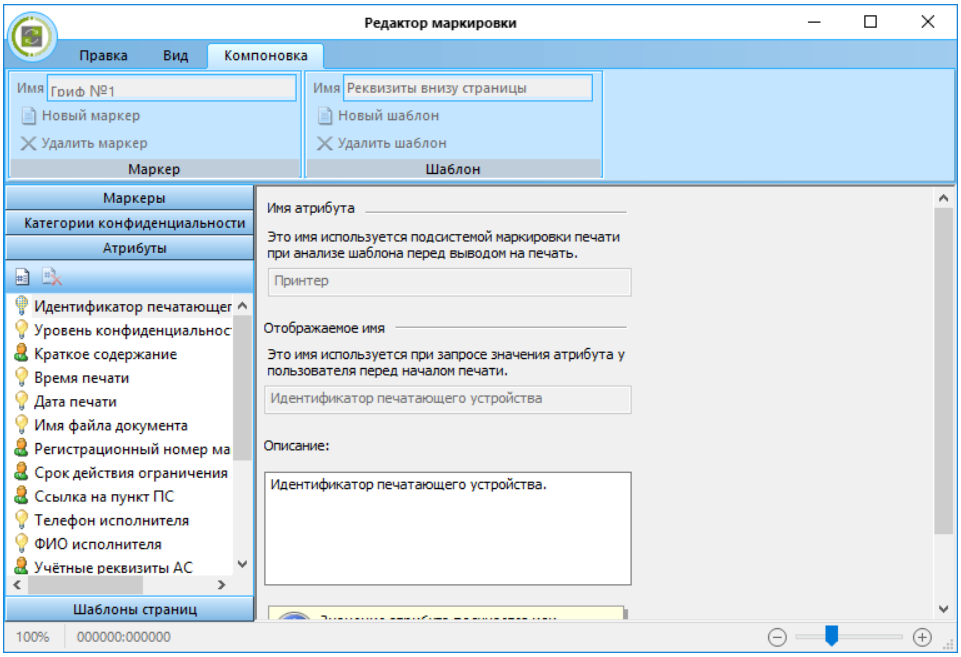
4 — Строка состояния

Содержит индикаторы масштаба и положения курсора, используемые при работе с шаблонами страниц

Порядок действий при редактировании маркеров

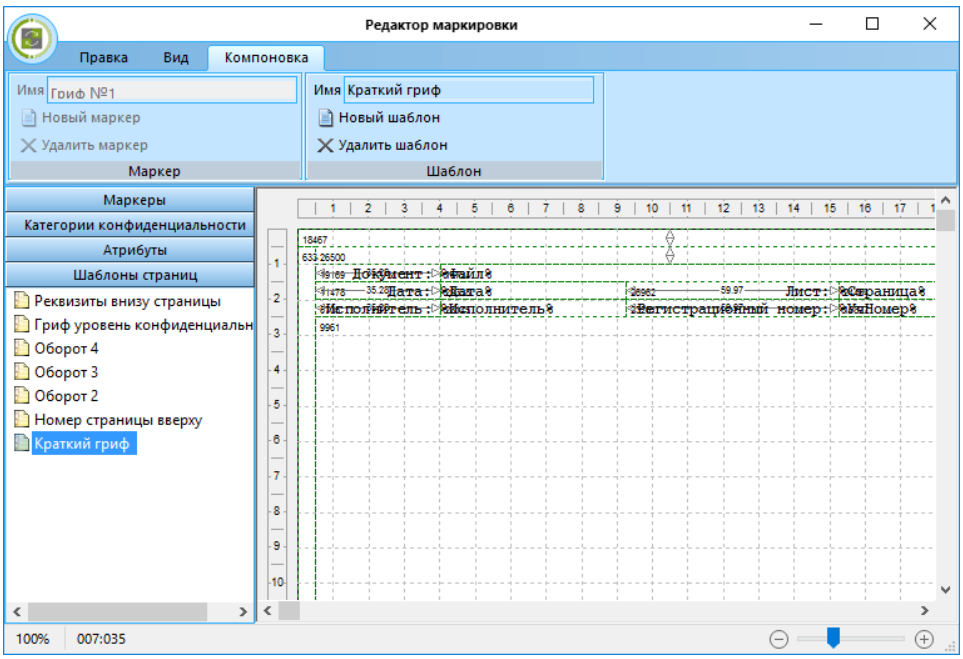
Редактирование маркеров в программе рекомендуется выполнять в следующем порядке:

1. В панели выбора объектов перейдите к разделу "Атрибуты".



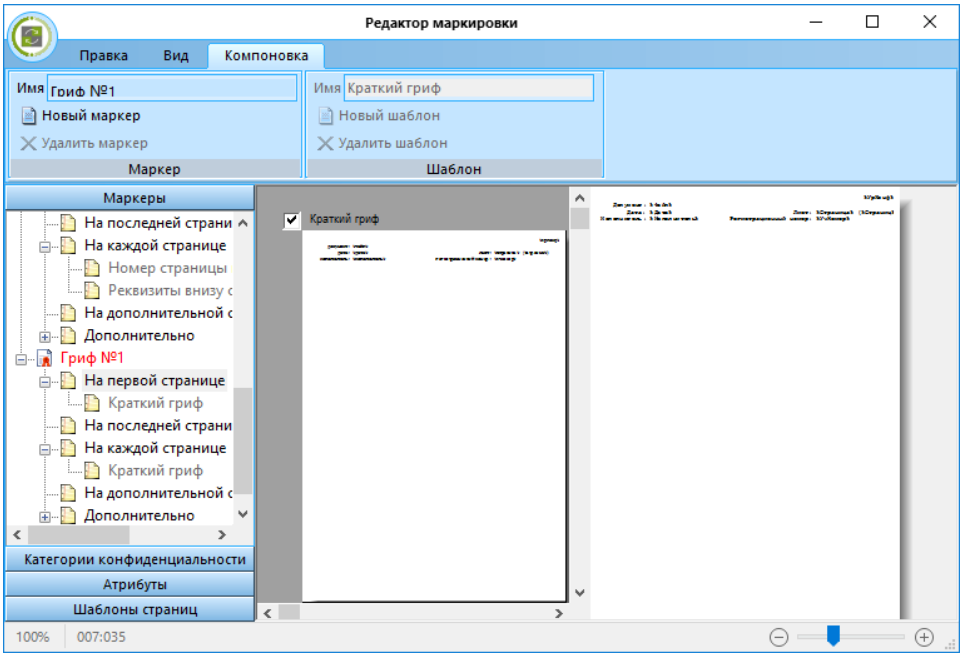
Если в списке отсутствуют нужные атрибуты (позволяющие получать и выводить необходимые сведения при печати документов), измените имеющиеся атрибуты или добавьте новые.

2. В панели выбора объектов перейдите к разделу "Шаблоны страниц".



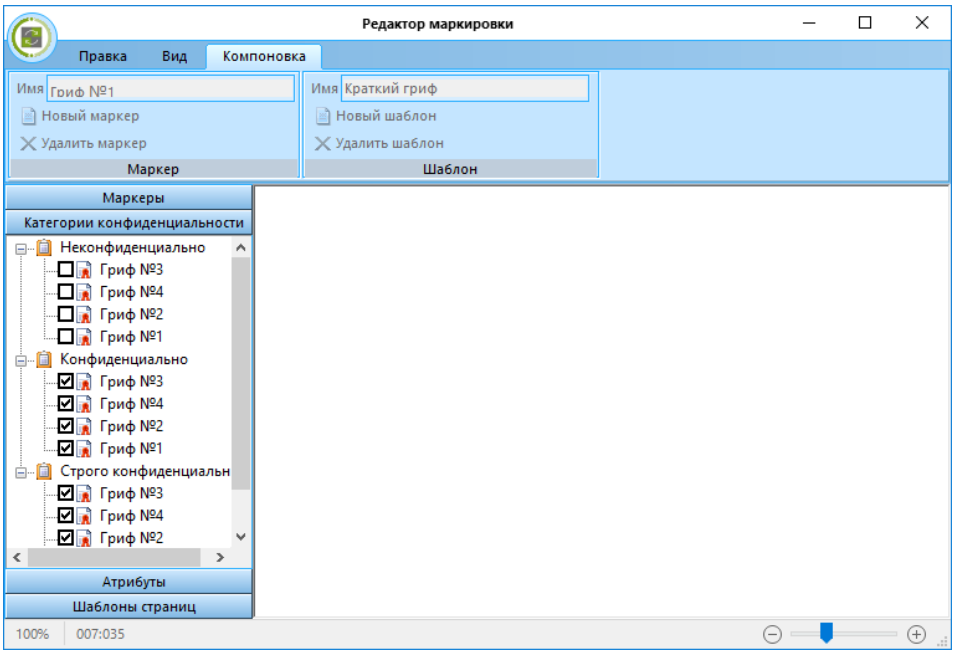
Если в списке отсутствуют нужные шаблоны (с требуемым оформлением и наборами атрибутов), измените имеющиеся шаблоны или добавьте новые. Редактирование элементов оформления шаблонов осуществляется стандартными способами.

3. В панели выбора объектов перейдите к разделу "Маркеры".



Если в списке отсутствуют нужные маркеры (с требуемыми названиями и компоновкой шаблонов), измените имеющиеся маркеры или добавьте новые. Для изменения компоновки шаблонов маркера выберите нужную страницу (диапазон страниц) и в левой части области редактирования отметьте нужные шаблоны.

4. В панели выбора объектов перейдите к разделу "Категории конфиденциальности".



Для каждой категории конфиденциальности отметьте маркеры, которые будут использоваться при печати документов.

5. Сохраните сделанные изменения. Для этого вызовите общее меню программы с помощью кнопки в левом верхнем углу окна и выберите команду "Сохранить описание маркировки".

6. Закройте программу.

Глава 10
Настройка контроля целостности ресурсов и замкнутой программной среды

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

Механизм ЗПС предназначен для ограничения 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, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале безопасности регистрируются события несанкционированного доступа (НСД).

В системе Secret Net Studio настройка механизма КЦ может осуществляться совместно с настройкой механизма ЗПС. Для этих механизмов используется общее средство настройки — программа "Контроль программ и данных". В данной главе рассматривается порядок работы с программой для реализации контроля целостности отдельно или совместно с механизмом ЗПС.

Общие сведения о методах и средствах настройки

Модель данных

Параметры, определяющие работу механизмов КЦ и ЗПС, объединены в рамках единой модели данных. **Модель данных (МД)** представляет собой иерархию объектов и описание связей между ними. В модели используются 5 категорий объектов:

Состав

Объект	Пояснение
Ресурс	Описание файла или каталога, переменной реестра или ключа реестра Windows. Однозначно определяет место нахождения контролируемого ресурса и его тип
Группа ресурсов	Объединяет несколько описаний ресурсов одного типа (файлы, каталоги, объекты системного реестра, исполняемые скрипты). Например, исполняемые файлы или ключи реестра, относящиеся к конкретному приложению. Однозначно определяется типом ресурсов, входящих в группу
Задача	Набор групп ресурсов одного и того же или разных типов. Например, задача может одновременно включать группу системных файлов и группу объектов системного реестра Windows
Задание	Определяет параметры проведения контроля целостности. Например, методы контроля, алгоритмы расчета контрольных сумм, расписание проведения контроля, реакции системы на обнаруженные ошибки. Включает в себя набор задач и групп ресурсов, подлежащих контролю. Например, при использовании замкнутой программной среды может объединять описания исполняемых файлов, разрешенных для запуска определенной группе пользователей

Состав

Объект	Пояснение
Субъект управления	Компьютер и группа, включающая пользователей и компьютеры (при локальном управлении — также и отдельные пользователи). Определяет компьютеры, на которых выполняется контроль целостности в соответствии с назначенными заданиями, и пользователей, которым разрешено запускать программы, заданные заданиями ЗПС

Структура

Объекты одной категории являются подчиненными или вышестоящими по отношению к объектам другой категории. Так, ресурсы являются подчиненными по отношению к группам ресурсов, а группы — задачам. Включение ресурсов в группы, групп в задачи, а задач — в задания называется установлением связей между объектами. В конечном итоге задания назначаются субъектам. Модель, включающая в себя объекты всех категорий, между которыми установлены все нужные связи, — это подробная инструкция системе Secret Net Studio, определяющая, что и как должно контролироваться.

Пояснение. Модель также может содержать объекты, не связанные с другими, или неполные цепочки объектов, но работать будут только те фрагменты, которые объединяют все уровни модели.

Модель данных состоит из двух частей. Одна часть относится к ЗПС среде, другая — к КЦ. Набор заданий для каждой из этих частей модели свой. Задачи, группы ресурсов и ресурсы могут входить как в одну, так и в другую часть модели.

Хранение

ЛБД КЦ-ЗПС организована в виде набора файлов, хранящихся в подкаталоге каталога установки Secret Net Studio. В ЛБД КЦ-ЗПС на каждом компьютере хранится модель данных, относящаяся к этому компьютеру.

Для клиентов в сетевом режиме функционирования формируется ЦБД КЦ-ЗПС в специальном централизованном хранилище. Для организации централизованного управления создаются две модели данных — для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64-разрядными версиями операционных систем. Каждая из централизованных моделей данных является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности.

В централизованном режиме программы управления КЦ-ЗПС модели данных могут быть созданы с использованием тиражируемых и нетиражируемых заданий. Эти два вида заданий различаются способом формирования задач и местом расчета и хранения эталонов.

Задания	Особенности
Тиражируемые	Эталонные значения для таких заданий рассчитываются централизованно и хранятся в ЦБД КЦ-ЗПС. При синхронизации вместе с задачами эталонные значения тиражируются на указанные рабочие станции и сохраняются в ЛБД КЦ-ЗПС. Таким образом, эталоны ресурсов тиражируемого задания одинаковы на всех компьютерах, с которыми связано данное задание
Нетиражируемые	Для нетиражируемых заданий эталонные значения не тиражируются, а вычисляются на рабочих станциях и хранятся только в ЛБД КЦ-ЗПС

Формирование модели данных для ЗПС

Модель данных для механизма ЗПС можно сформировать на основе сведений о запускавшихся программах из журнала Secret Net Studio. Для этого при централизованном управлении необходимо создать файл журнала в dvt- или snlog-формате, содержащий выборку записей за интересующий период. Затем этот файл с помощью программы управления КЦ-ЗПС в централизованном режиме импортируется в базу данных КЦ-ЗПС. При использовании Локального центра управления КЦ-ЗПС сведения о запускавшихся программах можно загрузить непосредственно из локального журнала. Далее на основании этих данных формируются задания ЗПС для субъектов.

Объекты модели по умолчанию

Во время установки клиентского ПО системы Secret Net Studio проверяется наличие модели данных в БД КЦ-ЗПС. Если модель данных отсутствует, автоматически выполняется ее формирование и наполнение объектами по умолчанию.

При начальном формировании в модель добавляются следующие задания:

- "Задание для контроля ресурсов Secret Net Studio";
- "Задание для контроля реестра Windows";
- "Задание для контроля файлов Windows".

Задания включают готовые задачи с ресурсами, сформированными по предопределенному списку. Для этих заданий устанавливаются связи со следующими субъектами:

- в локальной модели — с субъектом "Компьютер";
- в централизованной модели — с субъектом КЦ SecretNetICheckDefault (для 32-разрядных ОС) или SecretNetIcheckDefault64 (для 64-разрядных ОС). Субъект содержит список компьютеров домена безопасности с ОС соответствующей разрядности и установленным клиентом Secret Net Studio.

Также в модель добавляются некоторые дополнительные задачи, не связанные с заданиями.

Программа управления КЦ-ЗПС

Для настройки механизмов КЦ и ЗПС используется программа "Контроль программ и данных" (далее — Программа управления КЦ-ЗПС), входящая в состав клиентского ПО системы Secret Net Studio.

Программа управления КЦ-ЗПС располагает как автоматическими, так и ручными средствами формирования элементов модели данных. Ручные методы можно использовать на любом уровне модели для формирования и модификации объектов и связей. Автоматические методы предпочтительнее при работе с большим количеством объектов, однако они требуют более тщательного контроля результатов. Для создания небольших фрагментов модели могут быть использованы ручные методы, что делает процесс более контролируемым и позволяет избежать случайных ошибок. В общем случае наиболее типичный путь состоит в комбинации этих двух методов.

Программа управления КЦ-ЗПС может работать в централизованном и локальном режимах. Централизованный режим используется для настройки параметров работы механизмов на компьютерах с установленным клиентом в сетевом режиме функционирования.

Для работы с программой управления КЦ-ЗПС пользователь должен входить в локальную группу администраторов компьютера. Чтобы использовать централизованный режим, пользователь дополнительно должен входить и в группу администраторов домена безопасности.

Описание программы приведено на стр.**275**.

Синхронизация центральной и локальной баз данных

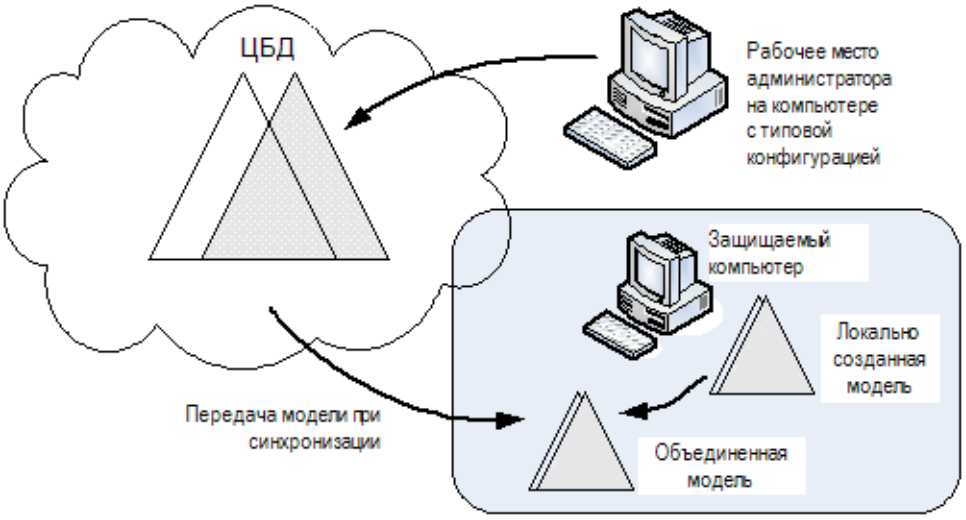
При синхронизации происходит передача изменений, внесенных в ЦБД КЦ-ЗПС, на все те компьютеры, к которым эти изменения относятся. Изменения сохраняются в ЛБД КЦ-ЗПС. Синхронизация может выполняться в следующие моменты:

- при загрузке компьютера;
- при входе пользователя в систему;
- после входа (в фоновом режиме во время работы пользователя);
- периодически через определенные интервалы времени;
- принудительно по команде администратора;

- непосредственно после внесения изменений в ЦБД КЦ-ЗПС.

Примечание. Чтобы синхронизация выполнялась незамедлительно при сохранении модели данных в ЦБД, необходимо разослать на компьютеры оповещения об изменениях. Запуск рассылки оповещений можно выполнять вручную или автоматически (см. стр. 132). Для оперативной синхронизации на компьютерах должны быть настроены определенные параметры ОС Windows (см. стр. 272).

В результате синхронизации в ЛБД КЦ-ЗПС формируется объединенная актуальная модель данных, включающая локально и централизованно созданные задания, а также связанные с ними задачи, группы ресурсов и ресурсы.



Защита от дублирования ресурсов при синхронизации

Если в ЛБД поступает из ЦБД описание ресурса, которое уже имеется в локальной модели данных, то в ЛБД остается только одно описание ресурса, но все связи ресурса сохраняются (суммируются). Если же этот ресурс снимается с контроля в ЦБД, то связи этого ресурса, имевшиеся в ЛБД ранее, восстанавливаются.

Начальная настройка механизмов

В этом разделе рассматривается порядок начальной настройки механизмов КЦ и ЗПС. В качестве основного метода настройки предлагается подход с максимальным использованием автоматических средств — мастера моделей данных и генератора задач.

Подготовка к построению модели данных

При подготовке к построению модели данных проводится анализ размещения ПО и данных на защищаемых компьютерах. Разрабатываются требования к настройке КЦ и ЗПС, включающие в себя:

- сведения о защищаемых компьютерах (установленное ПО, пользователи и их функциональные обязанности);
- перечень ресурсов, подлежащих контролю целостности;
- перечень программ, с которыми разрешено работать разным группам пользователей.

Из числа компьютеров с установленным клиентом в сетевом режиме функционирования выделяются группы с полным совпадением, частичным совпадением и с уникальной конфигурацией ПО и данных. Осуществляется подготовка рабочего места администратора для проведения настройки. На рабочем месте необходимо установить все программное обеспечение, описание ресурсов которого предполагается выполнять автоматическими средствами добавления задач в модель данных.

Примечание. Редактирование централизованных моделей данных осуществляется со следующими особенностями: для редактирования доступна та модель данных, которая соответствует разрядности ОС Windows на рабочем месте администратора. Модель данных другой разрядности доступна только для чтения (при этом можно экспортировать данные из этой модели в другую). Таким образом, если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места — на компьютере с 32-разрядной версией ОС Windows и на компьютере с 64-разрядной версией ОС.

Общий порядок настройки

Для использования на компьютерах механизмов КЦ и ЗПС выполните настройку в следующем порядке:

1. Сформируйте новую модель данных с настройкой контроля по умолчанию (см. стр.**116**).
2. Добавьте в модель данных дополнительные объекты:
   - задачи для КЦ и для использования в ЗПС (см. стр.**117**);
   - задания КЦ, ПАК "Соболь" или ЗПС (см. стр.**119**).

   Примечание. Для формирования задач и заданий ЗПС можно использовать метод накопления сведений о действиях пользователей во время работы. Данный метод предусматривает использование мягкого режима работы механизма и получение информации о запуске программ из журнала Secret Net Studio (см. стр.**121**).
3. При настройке механизма ЗПС:
   - установите связи заданий ЗПС с субъектами (см. стр.**123**);
   - укажите ресурсы для контроля (см. стр.**123**);
   - включите режим изоляции процессов (см. стр.**125**).
4. Создайте эталоны контролируемых ресурсов (см. стр.**126**).
5. При настройке механизма ЗПС:
   - для пользователей, при работе которых не должны действовать ограничения ЗПС, предоставьте привилегию (см. стр.**130**);
   - включите жесткий режим работы механизма ЗПС (см. стр.**130**).
6. При настройке механизма КЦ включите действие этого механизма (см. стр.**129**). Перед началом эксплуатации механизма рекомендуется выполнить проверку корректности параметров заданий контроля (см. стр.**131**).

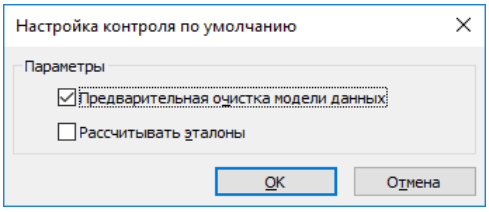
В процессе эксплуатации системы может возникнуть необходимость корректировки или пересмотра модели данных. Если предполагается кардинальная переработка модели, то лучше выполнить ее с нуля. Если переработке будет подвергнута небольшая часть модели, то в этом случае можно применить отдельные процедуры модификации модели (см. стр.**140**).

Формирование новой модели данных

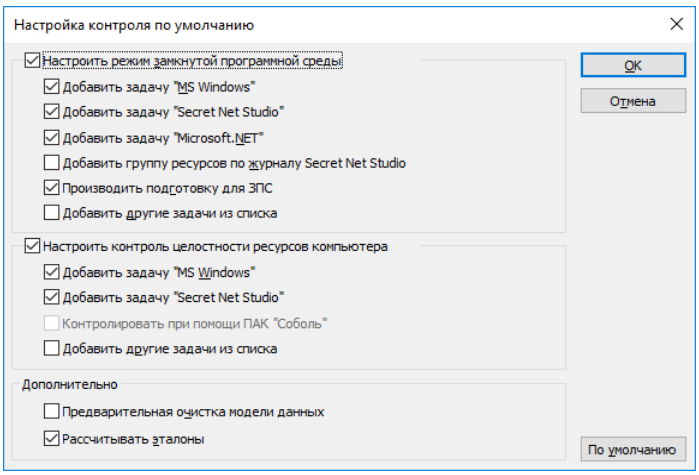
При формировании в модель данных автоматически добавляются описания для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ. Новая модель данных будет сформирована с настройкой контроля по умолчанию.

Для формирования новой модели данных:

1. В Центре управления КЦ-ЗПС выберите команду "Файл | Новая модель данных".
   - В централизованном режиме на экране появится диалог:



- В локальном режиме на экране появится диалог:



2. В зависимости от режима работы программы настройте нужные параметры и нажмите кнопку "OK".

- В централизованном режиме рекомендуется оставить заданные параметры без изменения.

  Предыдущая модель данных соответствующей разрядности ОС будет удалена. Затем начнется автоматическое формирование модели данных, и после успешного завершения в основном окне программы управления КЦ-ЗПС появятся новые элементы модели данных.

- В локальном режиме предоставляется возможность детальной настройки параметров для формирования новой модели данных. Помимо стандартных задач в модель можно добавить задачи, сформированные на основе ресурсов приложений. Добавление таких задач осуществляется с помощью параметра "Добавить другие задачи из списка".

  Примечание. Для механизма ЗПС рекомендуется оставить включенным параметр "Производить подготовку для ЗПС" для выполнения операции подготовки ресурсов. Ресурсы будут помечены признаком "выполняемый", и для исполняемых файлов будет выполнен поиск связанных с ними модулей. Это основное назначение данной операции, без нее настройка ЗПС будет неполноценной.

  После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура объектов.

Добавление задач в модель данных

Целью этого этапа настройки является дополнение модели данных фрагментом, включающим список других необходимых задач (помимо ресурсов Windows и Secret Net Studio). Для этого могут быть использованы как ручные методы, так и специальное средство — механизм генерации задач. Задачи создаются на основании сведений об установленных на компьютере программных продуктах. Для этого используются сведения MS Installer и ярлыки меню "Пуск" ОС Windows. Рекомендуется использовать механизм генерации при наполнении модели данных сложными задачами, включающими в себя большое количество ресурсов.

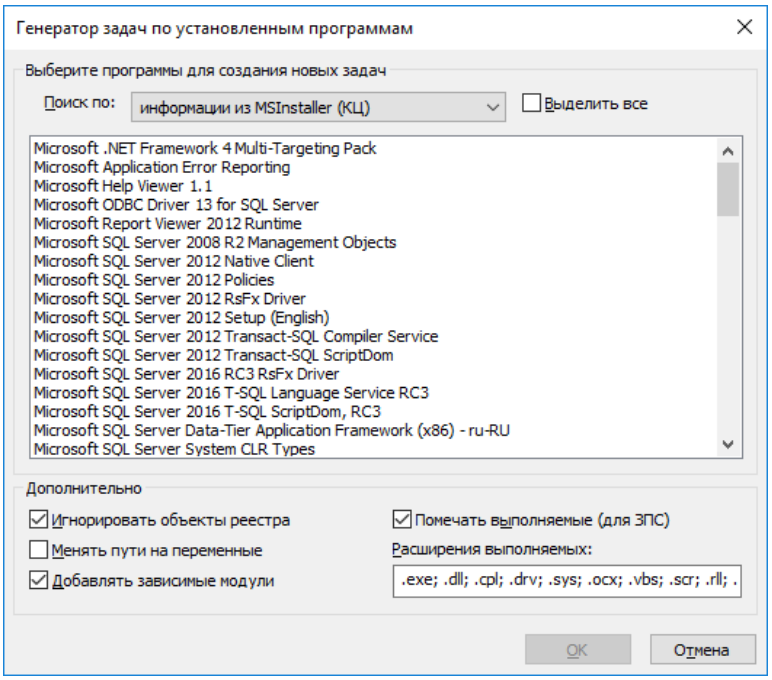
Перед началом генерации администратор безопасности может просмотреть список установленного ПО и наметить те компоненты (программы), для которых должны быть сгенерированы задачи. При этом в задачи будут автоматически включены ресурсы, связанные с исполняемыми модулями выбранного ПО. Можно также задать дополнительное условие фильтрации отбираемых ресурсов.

Кроме того, для ЗПС задачи можно добавить, используя способ формирования заданий ЗПС по журналу Secret Net Studio (см. стр.**121**).

Для добавления в модель задач с помощью механизма генерации:

1. В программе управления КЦ-ЗПС в меню "Сервис" выберите команду "Генератор задач".

   На экране появится диалог.



   Диалог предназначен для выбора программ, а также задания дополнительных условий отбора ресурсов.

2. Укажите в поле "Поиск по" — из какого списка должны выбираться программы.

3. Выберите в списке программы и укажите в нижней части диалога дополнительные условия отбора ресурсов.

Совет. Для выделения нескольких программ используйте клавишу <Ctrl>. Для выделения всего списка поставьте отметку в поле "Выделить все".

Условие	Пояснение
Игнорировать объекты реестра	Ресурсы, являющиеся объектами реестра, в задачи не включаются
Менять пути на переменные	При записи в модель данных абсолютные пути к файлам и каталогам меняются на имена переменных окружения

Условие	Пояснение
Добавлять зависимые модули	Зависимые модули — это файлы, от которых зависит исполнение исходных файлов. Например, это могут быть драйверы и библиотеки, не входящие непосредственно в запускаемые пользователем приложения, но без которых работа этих приложений невозможна. Зависимые модули добавляются в ту же группу ресурсов, где находится исходный файл. Включение зависимых модулей в список осуществляется рекурсивно: файлы, от которых зависит исполнение самих зависимых модулей, также включаются в список
Помечать выполняемые (для ЗПС)	Выполняемые файлы при отображении в окне программы управления КЦ-ЗПС помечаются специальным значком. К выполняемым относятся файлы, имеющие расширения, указанные в строке "Расширения выполняемых", а также файлы с нетипичными расширениями (список таких файлов формируется в параметрах программы — см.стр.280). При необходимости отредактируйте список расширений для применения при этом отборе ресурсов

Примечание. При выборе из списка MS Installer можно задать каждое из приведенных выше дополнительных условий. При выборе по ярлыкам из меню "Пуск" можно задать только два условия: "менять пути на переменные" и "помечать выполняемые".

4. Нажмите кнопку "ОК".

   Начнется процесс генерации. Затем появится сообщение о его успешном завершении.

5. Нажмите кнопку "ОК" в окне сообщения.

   В модель добавятся новые задачи, включающие в себя группы ресурсов, но не связанные с вышестоящими объектами (заданиями), на что указывает значок  (верхняя половина кружка окрашена красным цветом).

Добавление заданий и включение в них задач

Цель данного этапа — сформировать задания на основе задач, созданных на предыдущем этапе.

Для заданий КЦ должна быть выполнена настройка, в которой указываются:

- методы и алгоритмы контроля защищаемых ресурсов;
- реакция системы в случае нарушения целостности ресурсов;
- перечень событий, регистрируемых в журнале;
- расписание, в соответствии с которым должна проводиться проверка.

Пояснение. Порядок настройки задания для ПАК "Соболь" описан на стр.157.

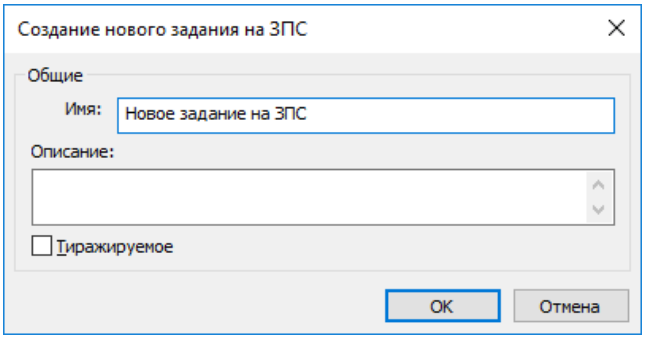
Для формирования задания ЗПС:

1. В программе управления КЦ-ЗПС выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание".

   На экране появится диалог выбора типа задания.

2. Выберите тип задания ЗПС и нажмите кнопку "ОК".

   На экране появится диалог:



3. Введите имя задания, его краткое описание и нажмите кнопку "OK".

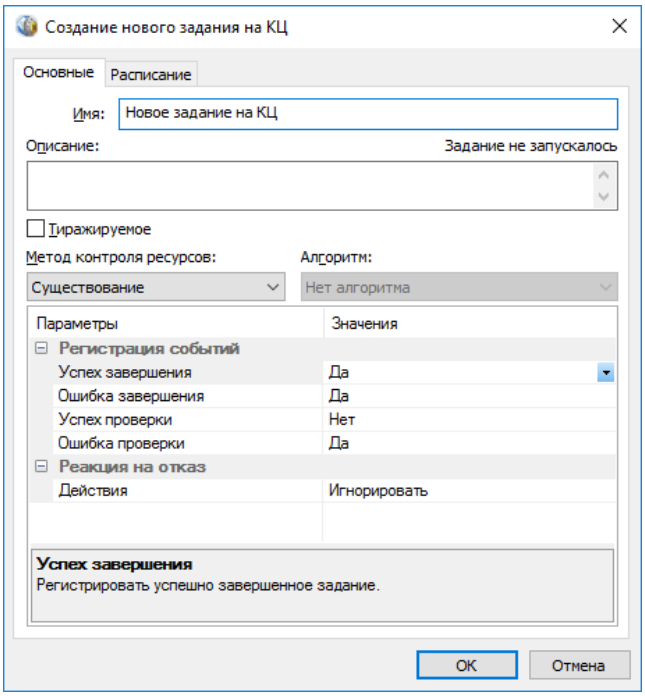
Для формирования задания КЦ:

1. В программе управления КЦ-ЗПС выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание".

   На экране появится диалог выбора типа задания.

2. Выберите тип задания КЦ и нажмите кнопку "OK".

   На экране появится диалог:



3. Введите имя и краткое описание задания КЦ.
4. Укажите метод контроля ресурсов, выбрав его из списка.

Внимание! Задания, созданные средствами централизованного управления, отображаются в программе, работающей в локальном режиме, полужирным шрифтом. Такие задания нельзя удалить из модели данных. В них нельзя включать задачи.

Включение задач в задание

Для включения задач в задание:

1. Выберите категорию "Задания" на панели категорий.
2. В окне структуры вызовите контекстное меню для задания и выберите команду "Добавить задачи/группы | Существующие".

   Появится диалог со списком всех задач и групп ресурсов, еще не включенных в данное задание.

3. Выберите задачи, включаемые в задание, и нажмите кнопку "OK".

Совет. Для выбора нескольких задач используйте клавишу <Ctrl> или поле "Выделить все".

Включение мягкого режима ЗПС и формирование заданий по журналу

При формировании заданий ЗПС на основе сведений из журнала Secret Net Studio действия выполняются в следующем порядке:

1. Включение ЗПС в мягком режиме (см. ниже).
2. Сбор сведений в журнале (см. стр.**121**).
3. Добавление задач ЗПС, созданных по журналу (см. стр.**122**).

Включение ЗПС в мягком режиме

Для работы ЗПС предусмотрены два режима работы: мягкий и 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.

Для включения ЗПС в мягком режиме:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. Установите отметку в следующих полях:
   - "Режимы заданы централизованно" (в случае централизованного управления);
   - "Режим ЗПС включен";
   - "Мягкий режим".
4. Нажмите кнопку "ОК".

Для выбранного компьютера (или группы) начнет действовать механизм ЗПС в мягком режиме.

Сбор сведений об используемых программах и скриптах в журнале

Модель ЗПС может быть создана на основе данных журнала Secret Net Studio. Чтобы собрать нужные сведения, пользователям разрешается запускать любые программы и скрипты. На это отводится некоторый период времени. Сведения о запускаемых программах и скриптах регистрируются в журнале. На время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых замкнутая программная среда будет использоваться.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о программах и скриптах из журнала Secret Net Studio. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net Studio или из файла, в который предварительно были сохранены записи журнала.

Пояснение. Описание процедур сохранения записей журнала приведено в разделе "Экспорт записей локальных журналов" на стр.55

Добавление задач ЗПС, созданных по журналу

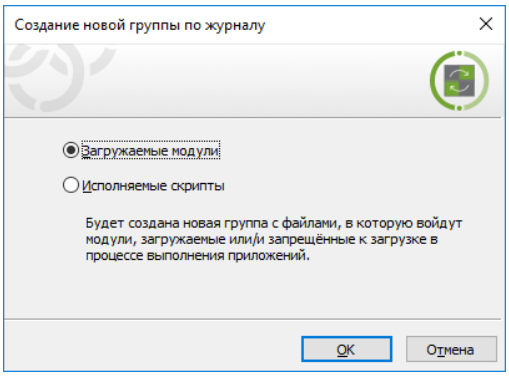
На этой стадии на основании данных из журнала Secret Net Studio формируются задачи, добавляемые к заданиям ЗПС.

Примечание. Источником при добавлении задач ЗПС по журналу в централизованном режиме является dvt- или snlog-файл, в который предварительно были экспортированы сведения из журнала. В локальном режиме источником может быть журнал безопасности или журнал Secret Net Studio.

Для добавления задач ЗПС, созданных по журналу:

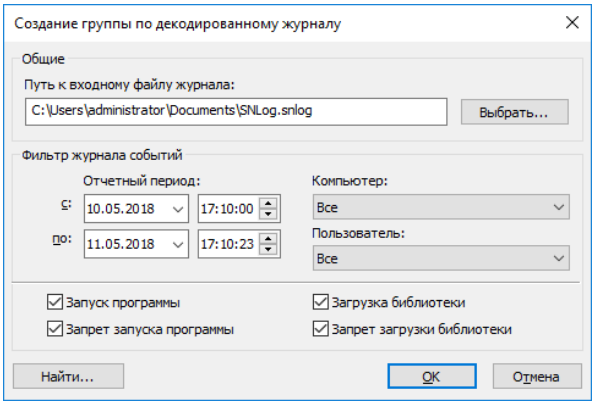
1. В основном окне программы управления КЦ-ЗПС выберите нужный субъект.
2. Выберите ранее созданное задание ЗПС, связанное с выбранным субъектом, или создайте новое задание ЗПС.
3. Вызовите контекстное меню и выберите в нем "Добавить задачи/группы | Новую группу по журналу".

   На экране появится диалог для выбора типа ресурсов, которые будут определены по записям журнала — загружаемые модули приложений или исполняемые скрипты.



4. Выберите нужный тип ресурсов для получения из журнала:
   - "Загружаемые модули" — если группа должна содержать файлы, которые загружались при работе приложений;
   - "Исполняемые скрипты" — если группа должна содержать скрипты, о загрузке которых имеются сведения в журнале.
5. Нажмите кнопку "OK".

   На экране появится диалог, подобный следующему.



6. Укажите необходимые значения параметров (путь к dvt- или snlog-файлу при работе в централизованном режиме или тип журнала при работе в локальном режиме, а также дополнительные условия отбора, если необходимо) и нажмите кнопку "OK".

К заданию будет добавлена группа ресурсов, сформированная на основании данных журнала.

Повторите эту процедуру и для других субъектов.

Установление связей субъектов с заданиями ЗПС

На данном этапе необходимо назначить субъектам сформированные задания ЗПС. Задания назначаются субъектам "Компьютер" и "Группа" (в локальном режиме — "Компьютер", "Пользователь" и "Группа пользователей"). Для того чтобы назначить задания нужным субъектам, их необходимо добавить в модель данных. В централизованной модели должны присутствовать субъекты, соответствующие компьютерам с уникальным составом ПО, и группы, включающие компьютеры со сходным составом ПО.

Для добавления субъекта в модель данных:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".

   На экране появится диалог для выбора типа субъектов (в централизованном режиме) или стандартный диалог ОС Windows для выбора пользователей и групп пользователей (в локальном режиме).
3. Укажите тип добавляемых объектов и затем найдите и выберите нужные объекты из числа существующих или, если добавляется группа компьютеров, укажите имя группы, ее описание и сформируйте список относящихся к ней компьютеров.
4. Нажмите кнопку "ОК".

   В окне программы управления КЦ-ЗПС появятся новые субъекты, отмеченные знаком ❗ (т. е. не связанные с другими объектами).

Для установления связи субъекта с заданием:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Найдите в дополнительном окне структуры или в области списка субъект, с которым требуется связать задание, вызовите контекстное меню и выберите команду "Добавить задания | Существующие".

   На экране появится диалог, содержащий список имеющихся заданий. Для каждого задания в списке указано количество субъектов, с которыми оно связано.
3. Выберите задания ЗПС, которые требуется назначить субъекту.

   Совет. Для выделения нескольких заданий используйте клавишу <Ctrl> или поставьте отметку в поле "Выделить все".
4. Нажмите кнопку "ОК".

Выбранные задания будут назначены субъекту.

Подготовка ресурсов для ЗПС

Чтобы ресурсы контролировались механизмом ЗПС, они должны иметь признак "выполняемый" и входить в задание ЗПС. Присвоение ресурсам признака "выполняемый" называется подготовкой ресурсов для ЗПС. Этот признак присваивается всем файлам, имеющим заданные расширения.

Также для каждого ресурса, которому установлен признак "выполняемый", может выполняться поиск зависимых модулей (см. стр. 156). Найденные зависимые модули добавляются в модель данных в те же группы ресурсов, в которые входят исходные модули. Им также присваивается признак "выполняемый".

Файлы, имеющие признак "выполняемый" и входящие в задание ЗПС, образуют список разрешенных для запуска программ. После связывания задания с пользователем и включения мягкого или жесткого режима система Secret Net Studio начнет контролировать запуск программ пользователем и регистрировать соответствующие события в журнале.

При построении модели данных с помощью автоматизированных средств (см. стр.**117**) подготовка ресурсов для ЗПС включена в соответствующие процедуры и выполняется по умолчанию. При построении модели вручную и ее модификации подготовка ресурсов для ЗПС выполняется как отдельная процедура.

В некоторых случаях (например, при ручном формировании заданий ЗПС или после добавления в модель новых ресурсов) может потребоваться заново построить список ресурсов, имеющих признак "выполняемый". Для этой цели в процедуре подготовки ресурсов предусмотрены две дополнительные возможности:

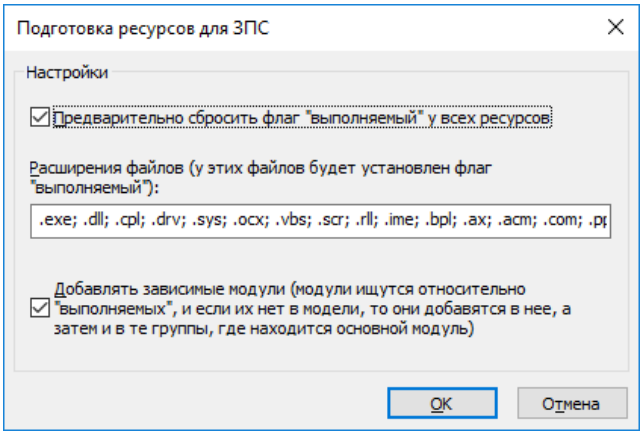
- Перед началом выполнения процедуры можно сбросить признак "выполняемый" у всех ресурсов в модели данных, у которых он имеется. В этом случае будут анализироваться все ресурсы, включенные в модель.
- Необходимо выполнить поиск зависимых модулей. В этом случае для каждого ресурса, которому будет установлен признак "выполняемый", будет проведен поиск в ресурсах компьютера зависимых модулей. Найденные зависимые модули будут добавлены в модель данных в те же группы ресурсов, в которые входят исходные модули.

Примечание. В централизованном режиме работы программы для выполнения процедуры подготовки ресурсов необходимо наличие в модели данных хотя бы одного задания ЗПС с ресурсами для контроля.

Для подготовки ресурсов:

1. Выберите в меню "Сервис" команду "Ресурсы ЗПС".

   На экране появится диалог для настройки параметров процедуры.



2. Если требуется, чтобы в ходе подготовки были проанализированы все имеющиеся в модели ресурсы (в том числе и те, у которых ранее был установлен признак "выполняемый"), оставьте отметку в поле "Предварительно сбросить флаг "выполняемый" у всех ресурсов". В этом случае список ресурсов, имеющих признак "выполняемый", будет построен заново. При этом время выполнения процедуры будет зависеть от общего числа ресурсов в модели данных.

   Если требуется, чтобы были проанализированы только ресурсы, не имеющие признака "выполняемый", удалите отметку.

3. Удалите из списка или добавьте в него расширения файлов, для которых должен быть установлен признак "выполняемый".
4. Для добавления в модель данных зависимых модулей оставьте отметку в поле "Добавлять зависимые модули".

   Если добавление зависимых модулей не требуется, удалите отметку.

5. Нажмите кнопку "OK".

Начнется процесс подготовки ресурсов к использованию в механизме ЗПС и появится информационное окно, отображающее ход выполнения процесса. После окончания появится сообщение об успешном завершении процесса.

Включение и настройка изоляции процессов

При необходимости обеспечить изолированную среду для определенных процессов (запретить обмен данными с другими процессами) действия выполняются в следующем порядке:

1. Включение режима изоляции процессов (см. ниже).
2. Добавление файлов изолируемых процессов в список ресурсов (см. стр.**125**).
3. Включение изоляции для ресурсов (см. стр.**126**).

Включение режима изоляции процессов

По умолчанию режим изоляции процессов отключен. Включение режима выполняется для субъекта управления.

Для включения режима изоляции:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. Установите отметку в поле "Изоляция процессов включена".
4. Нажмите кнопку "OK".

Для выбранного компьютера (или группы) начнет действовать режим изоляции процессов.

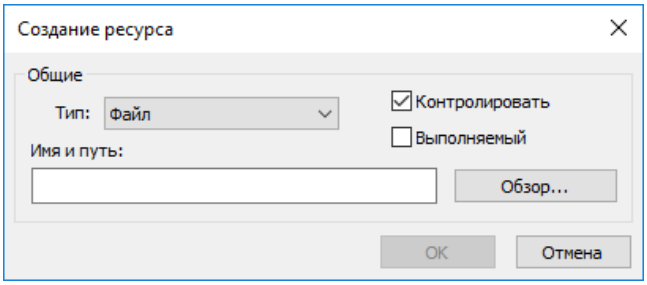
Добавление файлов изолируемых процессов в список ресурсов

В списки ресурсов заданий для ЗПС необходимо добавить исполняемые файлы процессов, которые будут изолированными. Изоляцию можно включить для файлов с расширением .exe (например, файл запуска редактора "Блокнот" notepad.exe), а также для файлов, перечисленных в списке "Имена исполняемых модулей процессов" в параметрах программы — см.стр.**280**.

Для добавления файла процесса в список ресурсов:

1. Вызовите контекстное меню группы ресурсов для файлов и каталогов в задании ЗПС и выберите в нем "Добавить ресурсы | Новый одиночный".

   Появится диалог для настройки параметров ресурса.



2. Укажите параметры добавляемого ресурса (см. таблицу ниже) и нажмите кнопку "OK".

Параметр	Пояснение
Тип	Укажите тип добавляемого ресурса: файл
Имя и путь	Введите вручную имя и полный путь к добавляемому ресурсу или нажмите кнопку "Обзор" и воспользуйтесь стандартной процедурой ОС
Контролировать	Отметка, установленная в этом поле, означает, что после включения механизма контроля целостности данный ресурс будет контролироваться. Если контроль данного ресурса не требуется, удалите отметку. В этом случае описание ресурса сохранится в модели данных и его можно будет поставить на контроль позднее
Выполняемый	Параметр используется для обозначения исполняемых файлов, которые формируют списки программ, разрешенных для запуска при включенной замкнутой программной среде

Ресурс появится в списке основного окна программы.

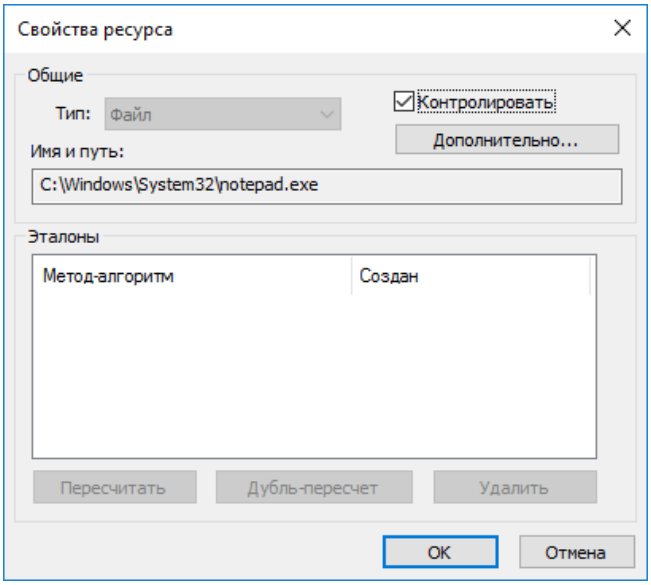
Включение изоляции для ресурсов

После добавления файлов процессов в список ресурсов выполняется процедура включения изоляции для каждого ресурса.

Для включения изоляции для ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог настройки параметров ресурса.



2. Нажмите кнопку "Дополнительно". В появившемся диалоге "Дополнительные свойства приложения" установите отметку в поле "Изолировать процесс" и нажмите кнопку "OK".
3. Нажмите кнопку "OK" в диалоге настройки параметров ресурса.

Расчет эталонов

Расчет эталонов необходим для контролируемых ресурсов, входящих в задания КЦ, а также и в задания ЗПС, если предусмотрен контроль целостности разрешенных для запуска программ. Процедура расчета выполняется автоматически, если модель данных создается с помощью мастера (см. стр. **116**). Если построение модели осуществляется с использованием генератора задач или вручную, расчет эталонов должен выполняться отдельно.

На этапе настройки целесообразно применять следующие способы расчета эталонов:

- расчет эталонов всех контролируемых ресурсов локальной модели данных (в централизованном режиме работы программы управления КЦ-ЗПС в этом случае происходит расчет эталонов только тех ресурсов, которые относятся к тиражируемым заданиям);
- расчет эталонов контролируемых ресурсов, относящихся к определенному заданию.

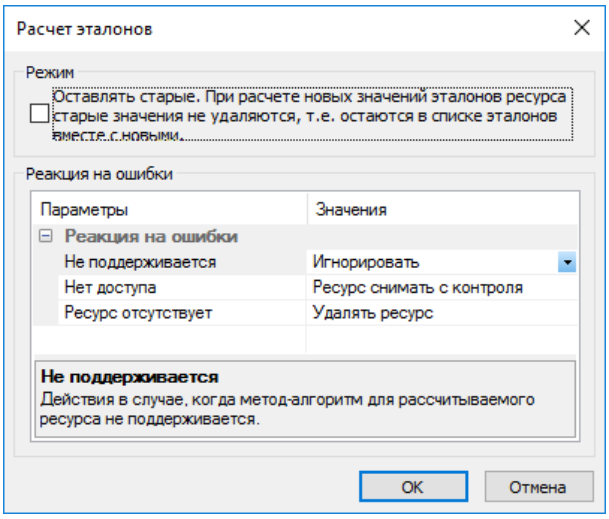
В локальном режиме расчет эталонов может быть выполнен для всех ресурсов, имеющихся в локальной модели данных. Исключение составляют те ресурсы, эталоны которых рассчитаны централизованно (ресурсы входят в тиражируемые задания).

В централизованном режиме используются различные методы для расчета эталонов тиражируемых и нетиражируемых заданий. Расчет эталонов тиражируемых заданий выполняется аналогично, как и в локальном режиме (эти эталоны будут затем переданы на компьютеры). Эталоны ресурсов для новых нетиражируемых заданий рассчитываются на компьютерах автоматически после передачи их в ЛБД при синхронизации. Если в нетиражируемое задание были внесены изменения, администратор может использовать команду для инициирования процесса расчета эталонов.

Для расчета эталонов в локальном режиме:

1. В зависимости от того, для каких ресурсов требуется рассчитать эталоны, выполните соответствующее действие:
   - чтобы выполнить расчет эталонов всех контролируемых ресурсов модели данных — выберите в меню "Сервис" команду "Эталоны | Расчет";
   - чтобы выполнить расчет эталонов ресурсов отдельного задания — вызовите контекстное меню этого задания и выберите команду "Расчет эталонов".

   На экране появится диалог "Расчет эталонов".



2. Если требуется сохранить предыдущие значения эталонов, установите отметку в поле "Оставлять старые".

   Примечание. Необходимость сохранения прежних ("старых") эталонных значений может возникнуть, например, при контроле содержимого файлов, изменяемых при автоматическом обновлении ПО. Дополнительные сведения об этом см. на стр. 154.

3. Настройте реакцию системы защиты на возможные ошибки при расчете эталонов. Для этого в левой части таблицы выберите вид ошибки, а в правой выберите нужную реакцию системы.

   Ошибки могут быть следующих видов:

   - метод/алгоритм расчета для данного ресурса не поддерживается;

- к ресурсу нет доступа на чтение или он заблокирован;
- ресурс по указанному пути не найден.

Для каждого вида ошибки можно задать одну из реакций, перечисленных в таблице ниже.

Реакция	Описание
Игнорировать	Реакция системы на ошибку отсутствует
Выводить запрос	При возникновении ошибки система выводит соответствующее сообщение и запрос на выполнение последующих действий
Удалять ресурс	При возникновении ошибки ресурс удаляется из модели данных
Ресурс снимать с контроля	Ресурс снимается с контроля, но остается в модели данных. При этом нужно учитывать, что ресурс будет снят с контроля не только в том задании, где выявлена ошибка, но и во всех остальных заданиях, с которыми ресурс связан

4. Нажмите кнопку "OK".

Начнется расчет эталонов. Ход выполнения расчета отображается в специальном окне полосой прогресса.

Если в процессе расчета обнаруживается ошибка и в качестве реакции на нее установлено значение "Выводить запрос", процедура будет приостановлена, и на экране появится запрос на продолжение процедуры.

Предусмотренные варианты продолжения процедуры перечислены в следующей таблице.

Вариант	Описание
Игнорировать	Процедура расчета будет продолжена. Реакция системы на ошибку отсутствует. Ресурс, вызвавший ошибку, остается в составе задачи (или задач). При проверке целостности ресурса будет регистрироваться событие тревоги с соответствующей реакцией (кроме варианта контроля по алгоритму "встроенная ЭЦП", если в файле отсутствует встроенная цифровая подпись на момент расчета эталона — в этом случае ресурс будет игнорироваться при контроле)
Снять с контроля	Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, остается в составе задачи (или задач), снимается с контроля и не проверяется во всех заданиях, в которые входит
Удалить	Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, автоматически удаляется из модели данных
Прервать	Процедура расчета будет прервана. Для расчета эталонов следует устранить причину, вызвавшую ошибку, и заново запустить процедуру расчета

5. Для выбора варианта продолжения процедуры нажмите соответствующую кнопку в окне сообщения.

В зависимости от выбранного варианта процедура будет продолжена или прервана, в каждом из этих случаев на экране появится сообщение.

6. Примите к сведению содержание сообщения и нажмите кнопку "OK".

Для расчета эталонов тиражируемых заданий (в централизованном режиме):

1. В зависимости от того, для каких ресурсов требуется рассчитать эталоны, выполните соответствующее действие:

- чтобы выполнить расчет эталонов всех тиражируемых заданий — выберите в меню "Сервис" команду "Эталоны | Расчет";

- чтобы выполнить расчет эталонов ресурсов отдельного тиражируемого задания — вызовите контекстное меню этого задания и выберите команду "Локальный расчет эталонов".

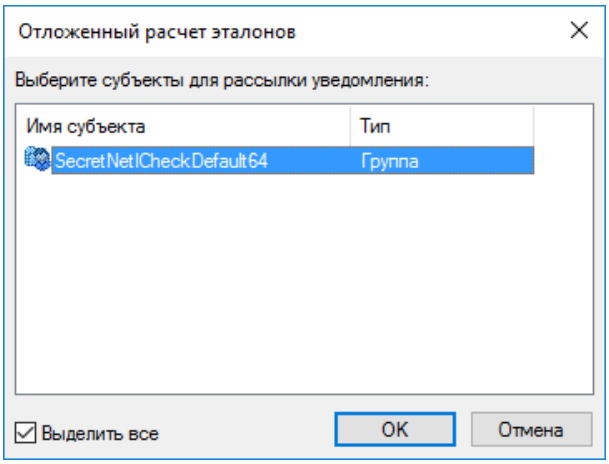
На экране появится диалог "Расчет эталонов".

2. Выполните действия, описанные в процедуре расчета эталонов в локальном режиме, начиная с шага **2** (см. выше).

Для расчета эталонов нетиражируемого задания (в централизованном режиме):

1. Вызовите контекстное меню нетиражируемого задания и выберите нужную команду:
   - чтобы отложить расчет эталонов нетиражируемого задания до следующей синхронизации ЦБД и ЛБД на компьютерах — выберите команду "Отложенный расчет эталонов";
   - чтобы инициировать незамедлительный расчет эталонов — выберите команду "Удаленный расчет эталонов".

   На экране появится диалог для выбора субъектов. Диалог содержит список субъектов, с которыми связано выбранное задание.



2. Выделите субъекты, на компьютерах которых требуется выполнить расчет эталонов для ресурсов данного задания. Нажмите кнопку "OK".

Примечание. Незамедлительный расчет эталонов (по команде "Удаленный расчет эталонов") следует выполнять только для компьютеров, включенных в данный момент. Если компьютер отключен, для расчета эталонов нетиражируемых заданий на этом компьютере можно использовать команду "Отложенный расчет эталонов" или выполнить на этом компьютере расчет эталонов в локальном режиме.

Включение механизма КЦ

Действие механизма КЦ включается при установлении связи заданий контроля целостности с субъектами "Компьютер" или "Группа" (компьютеров). При управлении в централизованном режиме включение механизма на компьютере произойдет после синхронизации ЛБД данного компьютера с ЦБД.

Для включения механизма контроля целостности:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите в нем команду "Добавить задания | Существующие".

   Появится диалог, содержащий список заданий контроля целостности. Для каждого задания в списке указано количество субъектов управления, с которыми оно связано.
3. Выберите задания, назначаемые субъекту, и нажмите кнопку "OK".

Для данного компьютера (или группы) начнет действовать механизм КЦ.

Предоставление привилегии при работе в ЗПС

В Secret Net Studio предусмотрена привилегия, которая отменяет ограничения ЗПС для пользователя. На пользователей, которым предоставлена данная привилегия, действие механизма замкнутой программной среды не распространяется.

По умолчанию привилегией обладают пользователи, входящие в локальную группу администраторов.

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для предоставления привилегии:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Замкнутая программная среда".
3. Для параметра "Учетные записи, на которые не действуют правила замкнутой программной среды" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

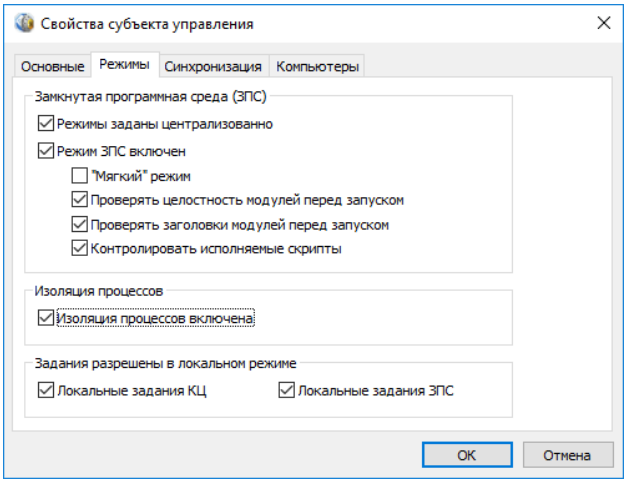
Включение жесткого режима ЗПС

В жестком режиме работы механизма ЗПС возможен запуск только разрешенных программ, библиотек и сценариев. Запуск других ресурсов блокируется, а в журнале Secret Net Studio регистрируются события тревоги как попытки несанкционированного доступа.

Параметры механизма ЗПС можно задать централизованно или локально. При этом в централизованном режиме доступна возможность задания параметров как для отдельных компьютеров, так и для групп компьютеров. Если заданы разные параметры механизма ЗПС для компьютера и для группы, в которую он входит, — на компьютере будут действовать все включенные параметры этих субъектов (параметры "суммируются"). Например, если для группы включен параметр "Мягкий режим", этот режим будет действовать на компьютере, даже если тот же параметр будет отключен для самого компьютера.

Для включения механизма ЗПС в жестком режиме:

1. В программе управления КЦ-ЗПС выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".



3. При работе в централизованном режиме установите отметку в поле "Режимы заданы централизованно".
4. Установите отметку в поле "Режим ЗПС включен" и удалите отметку из поля "Мягкий режим" (если она там установлена).
5. При необходимости установите дополнительные параметры контроля:

Параметр	Пояснение
Проверять целостность модулей перед запуском	При запуске программ, входящих в список разрешенных, проверяется их целостность
Проверять заголовки модулей перед запуском	В процессе контроля включается дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке
Контролировать исполняемые скрипты	Блокируется выполнение сценариев (скриптов), не входящих в перечень разрешенных для запуска и не зарегистрированных в базе данных системы Secret Net Studio

6. Нажмите кнопку "OK".

Проверка заданий

Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности параметров заданий. Проверка заключается в немедленном выполнении задания независимо от расписания. Такая проверка позволяет своевременно исправить ошибки, связанные с настройкой заданий.

Проверка выполняется отдельно для каждого задания. При этом для задания должны быть рассчитаны эталоны и оно должно быть связано с субъектом.

Для проверки задания предусмотрен облегченный режим и режим полной имитации. В облегченном режиме события в журнале не регистрируются и реакция на ошибки не отрабатывается. По завершении проверки выдается список обнаруженных ошибок. В режиме полной имитации события регистрируются и система отрабатывает реакцию на ошибки.

В локальном режиме работы программы проверку можно выполнить для любых заданий КЦ, связанных с компьютером (включая задания, созданные централизованно). В централизованном режиме возможна локальная проверка тиражируемых заданий, а также удаленная проверка любых централизованных заданий на включенных компьютерах выбранных субъектов.

Для запуска проверки в локальном режиме:

1. Выберите в меню "Сервис" команду "Запуск задания".

   На экране появится диалог со списком всех заданий контроля целостности.

2. Выберите в списке нужное задание. При необходимости проверки в режиме полной имитации установите отметку в поле "Полная имитация".
3. Нажмите кнопку "ОК".

Начнется выполнение задания, и по окончании будет выведено сообщение об успешном завершении или обнаруженных ошибках.

Для локальной проверки тиражируемых заданий (централизованный режим):

1. Выберите в меню "Сервис" команду "Запуск задания".

   На экране появится диалог со списком тиражируемых заданий контроля целостности.
2. Выполните действия, описанные в процедуре запуска проверки в локальном режиме, начиная с шага **2** (см. выше).

Для удаленной проверки задания (централизованный режим):

1. Вызовите контекстное меню задания и выберите команду "Удаленный запуск заданий".

   На экране появится диалог для выбора субъектов. Диалог содержит список субъектов, с которыми связано выбранное задание.
2. Выделите субъекты, на компьютерах которых требуется запустить проверку задания. Нажмите кнопку "ОК".

Начнется выполнение задания, и по окончании будет выведено сообщение об успешном завершении или обнаруженных ошибках.

Примечание. Удаленная проверка заданий может выполняться только для компьютеров, включенных в данный момент.

Сохранение и загрузка модели данных

Сохранение

Выполнив любые изменения в модели данных, ее текущее состояние можно сохранить в базе данных. Для сохранения модели выберите в меню "Файл" команду "Сохранить".

В централизованном режиме работы программы сохранение модели данных в ЦБД возможно при условии полного доступа к базе данных. Если полный доступ заблокирован (например, по причине запуска программы управления КЦ-ЗПС в централизованном режиме на другом компьютере), при попытке сохранения модели на экране появится сообщение о невозможности внесения изменений в базу данных. Программа в этом случае перейдет в режим доступа к ЦБД "только для чтения", в результате чего станет невозможно сохранить сделанные изменения в текущем сеансе. Возможность записи в ЦБД будет доступна только в следующем сеансе работы с программой.

Чтобы загрузить в следующем сеансе текущую редакцию модели данных, можно выполнить процедуру экспорта модели в файл, перезапустить программу и затем импортировать модель из файла (см. стр.**136**, стр.**137**).

Оповещение об изменениях

Сведения об изменениях в модели данных, выполненных в централизованном режиме, распространяются на включенные компьютеры домена в соответствии с настройкой параметра группы "Оповещения" (описание процедуры настройки параметров программы см. на стр.**280**). Функция действует для клиентов в сетевом режиме функционирования.

Если параметр имеет значение "Да", оповещение об изменениях в модели данных рассылается при каждом сохранении модели.

Если параметр имеет значение "Нет", оповещение не рассылается. При таком значении параметра оповещение можно разослать принудительно. Для принудительной рассылки оповещения выберите в меню "Сервис" команду "Оповестить об изменениях".

Настройка автоматического запуска синхронизации

При внесении изменений в ЦБД КЦ-ЗПС должна выполняться синхронизация этих изменений на компьютерах с последующим перерасчетом эталонных значений ресурсов (если это необходимо). Запуск синхронизации осуществляется локально на компьютерах в определенные моменты времени.

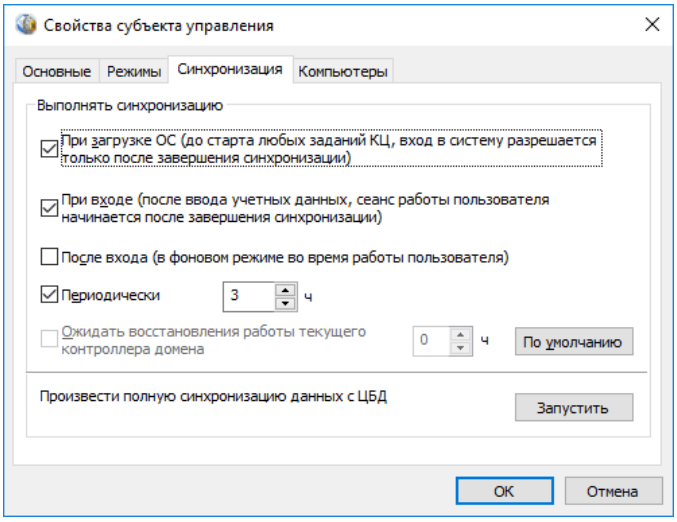
Настройка параметров запуска синхронизации осуществляется в централизованном режиме работы программы управления КЦ-ЗПС. Параметры могут быть заданы как для отдельных компьютеров, так и для групп. При этом действуют приоритеты применения параметров: наивысший приоритет имеют параметры компьютеров, затем параметры групп, кроме группы по умолчанию SecretNetICheckDefault, и, наконец, параметры самой группы по умолчанию. Например, если заданы разные параметры синхронизации для компьютера и для группы, в которую он входит, — на компьютере будут действовать только параметры компьютера.

Пояснение. Параметры групп, в которые включен компьютер, действуют в том случае, если в модели отсутствует субъект для этого компьютера со своими параметрами синхронизации. При этом между группами определен следующий порядок применения параметров: если компьютер включен в еще одну группу помимо группы по умолчанию SecretNetICheckDefault — на этом компьютере будут действовать параметры первой группы (не SecretNetICheckDefault). Если таких групп несколько и для них заданы разные параметры — применяются параметры группы по умолчанию.

Для своевременного выявления конфликтующих параметров синхронизации групп предусмотрена процедура проверки этих параметров. Проверку следует выполнять при наличии в модели нескольких групп, в которые могут быть включены одни и те же компьютеры.

Для настройки параметров запуска синхронизации:

1. В централизованном режиме программы управления КЦ-ЗПС выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Синхронизация".



3. Настройте параметры запуска процесса синхронизации. Описание параметров представлено в следующей таблице.

Параметр	Пояснение
При загрузке ОС...	Если установлена отметка, запуск синхронизации происходит при загрузке операционной системы до момента старта выполнения заданий КЦ. Таким образом, до начала выполнения на компьютере любых заданий КЦ они будут синхронизированы с ЦБД. При этом возможность входа пользователя в систему будет предоставлена только после завершения синхронизации. Действие данного параметра может приводить к задержкам входа при изменении в ЦБД объемных заданий и при низкой пропускной способности каналов связи
При входе...	Если установлена отметка, запуск синхронизации происходит после ввода пользователем своих учетных данных для входа в систему до момента старта выполнения заданий КЦ. Начало сеанса работы пользователя откладывается до завершения синхронизации. Действие данного параметра может приводить к задержкам входа при изменении в ЦБД объемных заданий и при низкой пропускной способности каналов связи
После входа...	Если установлена отметка, синхронизация выполняется в фоновом режиме после начала сеанса работы пользователя
Периодически	Если установлена отметка, запуск синхронизации происходит во время работы компьютера через указанный промежуток времени (в часах)
Ожидать восстановления работы текущего контроллера домена	*В текущей версии не используется*

Примечание. Если отключен автоматический запуск синхронизации (удалены отметки в полях "При загрузке ОС...", "При входе...", "После входа...." и "Периодически"), синхронизация на компьютере может выполняться только при поступлении оповещения об изменениях или по команде администратора. Для этого компьютер должен быть включен.

4. Нажмите кнопку "ОК".

Для проверки и корректировки параметров запуска синхронизации в группах:

1. В централизованном режиме программы управления КЦ-ЗПС выберите в меню "Сервис" команду "Проверить синхронизацию групп".

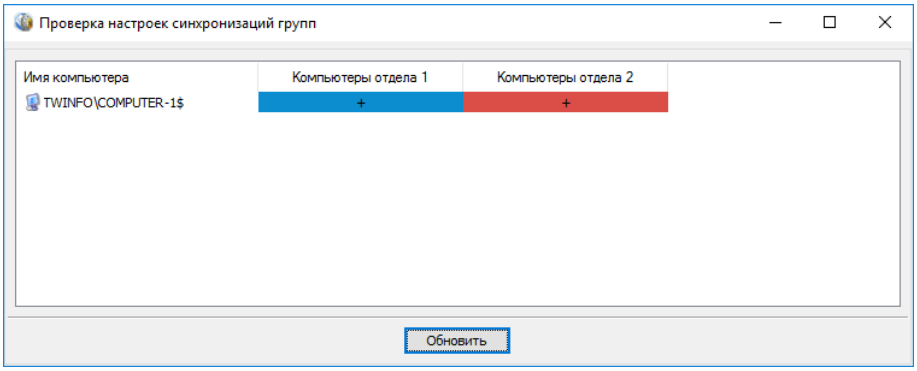
   Примечание. Команда недоступна, если список субъектов в модели данных содержит только одну группу по умолчанию SecretNetICheckDefault.

   Программа выполнит проверку вхождения компьютеров в группы с различными параметрами синхронизации. После проверки будут выведены сведения о результатах:

   - Сообщение об отсутствии обнаруженных конфликтов — если для всех компьютеров в группах отсутствуют несовпадающие параметры запуска синхронизации.

     Примечание. Не считается конфликтной ситуация, когда компьютер, включенный в группы с различными параметрами, также присутствует в модели и как отдельный субъект. В этом случае, в соответствии с приоритетом применения параметров, для этого компьютера будут применяться параметры, заданные для него как субъекта (независимо от того, какие параметры заданы для групп, в которые он входит).

   - Список компьютеров с конфликтующими параметрами:



В списке перечислены компьютеры и указаны группы, в которых заданы несовпадающие параметры запуска синхронизации для этих компьютеров.

2. Если в результате проверки показан список компьютеров с конфликтующими параметрами, переместите или сверните окно со списком. В основном окне программы выполните действия для устранения конфликтов (например, отредактируйте списки компьютеров в группах или добавьте указанные компьютеры в качестве отдельных субъектов со своими параметрами). Для повторной проверки снова перейдите в окно со списком и нажмите кнопку "Обновить".

Принудительный запуск полной синхронизации

Запуск синхронизации изменений ЦБД КЦ-ЗПС на компьютерах может выполняться автоматически в соответствии с заданными параметрами (см. стр.133). При работе с программой управления КЦ-ЗПС в централизованном режиме администратор может запустить внеочередной процесс полной синхронизации изменений ЦБД КЦ-ЗПС на определенных компьютерах.

Запуск синхронизации можно выполнить как для отдельных компьютеров, так и для групп. Однако при этом следует учитывать текущую загрузку каналов передачи данных, локальных и сетевых ресурсов. Без необходимости не следует запускать синхронизацию для групп компьютеров. Если в ЦБД хранится значительный объем данных, для полной синхронизации может потребоваться длительное время. В течение этого времени будут ограничены возможности работы пользователей на тех компьютерах, где проходит синхронизация.

Для запуска полной синхронизации:

1. В централизованном режиме программы управления КЦ-ЗПС выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Синхронизация".
3. Нажмите кнопку "Запустить".

   Произойдет запуск процесса синхронизации.

Загрузка и восстановление модели данных

Загрузка модели из базы данных осуществляется при каждом запуске программы управления КЦ-ЗПС или может быть выполнена по специальной команде в процессе работы.

Если вы вносите в модель изменения и не уверены в их правильности, не сохраняйте их сразу в БД. В этом случае будет возможность вернуться к варианту модели, сохраненной в БД. Для этого используется операция восстановления.

Для восстановления модели из базы данных:

1. В меню "Файл" выберите команду "Восстановить из базы".

На экране появится предупреждение о потере последних изменений.

2. Нажмите кнопку "Да" в окне предупреждения.

   Программа загрузит ранее сохраненную модель из базы данных.

Экспорт

Экспорт может осуществляться следующими способами:

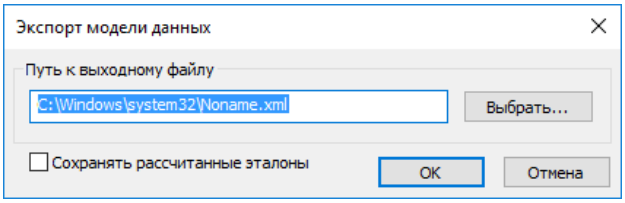
- экспорт всей модели данных;
- выборочный экспорт объектов определенных категорий (не применяется к объектам категории "Субъекты управления").

Примечание. Для автоматизации резервного копирования БД КЦ-ЗПС предусмотрена возможность экспорта и импорта модели данных путем запуска программы из командной строки. Описание параметров запуска приведено в приложении на стр.286.

Для экспорта текущей модели данных:

1. В меню "Файл" программы управления КЦ-ЗПС выберите команду "Экспорт модели в XML".

   На экране появится диалог настройки параметров экспорта.



2. В поле "Путь к выходному файлу" введите полное имя файла. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать...", чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
3. Если модель содержит ресурсы с рассчитанными эталонными значениями и требуется сохранить эти значения в файле, установите отметку в поле "Сохранять рассчитанные эталоны".

   Примечание. При включенном режиме экспорта ресурсов вместе с эталонными значениями программе потребуется сохранить текущую модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Сохранять рассчитанные эталоны".

4. Нажмите кнопку "OK" в диалоге настройки параметров экспорта.

Для выборочного экспорта объектов:

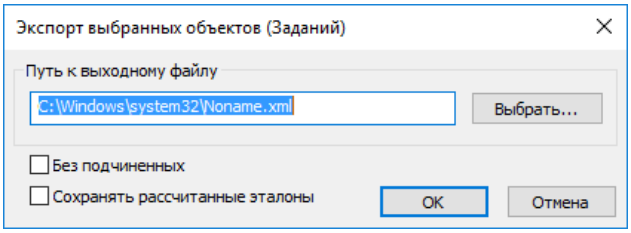
1. На панели категорий выберите категорию, в которой содержатся нужные объекты для экспорта (кроме категории "Субъекты управления").
2. В окне структуры или в области списка объектов найдите экспортируемые объекты.

   Предусмотрены следующие варианты выбора объектов:

   - все объекты, относящиеся к текущей категории, — для этого в окне структуры выберите корневой элемент с названием категории;
   - группа объектов, выбранных произвольным образом, — для этого в области списка объектов выделите нужные объекты, удерживая нажатой клавишу <Ctrl> или <Shift>;
   - отдельный объект в окне структуры или в области списка объектов.

3. Вызовите контекстное меню объекта (объектов) и выберите команду запуска процедуры экспорта. В зависимости от того, какие объекты были выбраны, эта команда имеет название: "Экспорт всех", "Экспорт содержимого папки" или "Экспорт выбранных".

   На экране появится диалог настройки параметров экспорта.



4. В поле "Путь к выходному файлу" введите полное имя файла. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге сохранения файла операционной системы Windows.
5. По умолчанию совместно с выбранными объектами экспортируются и те объекты, которые входят в цепочки связанных с ними объектов нижележащих уровней иерархии (например, задание — задача — группа ресурсов — ресурсы). Если требуется экспортировать только выбранные объекты, установите отметку в поле "Без подчиненных" (данное поле отсутствует в диалоге, если осуществляется экспорт ресурсов).
6. Если в числе экспортируемых объектов имеются ресурсы с рассчитанными эталонными значениями и требуется сохранить эти значения в файле, установите отметку в поле "Сохранять рассчитанные эталоны".

   Примечание. При включенном режиме экспорта ресурсов вместе с эталонными значениями программе потребуется сохранить текущую модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Сохранять рассчитанные эталоны".
7. Нажмите кнопку "OK" в диалоге настройки параметров экспорта.

Импорт

Процедура импорта из файла может выполняться следующими способами:

- общий импорт объектов в модель данных — позволяет импортировать все данные, хранящиеся в файле;
- импорт объектов в текущую категорию (не применяется к категории "Субъекты управления") — позволяет импортировать из файла объекты, относящиеся к той же категории.

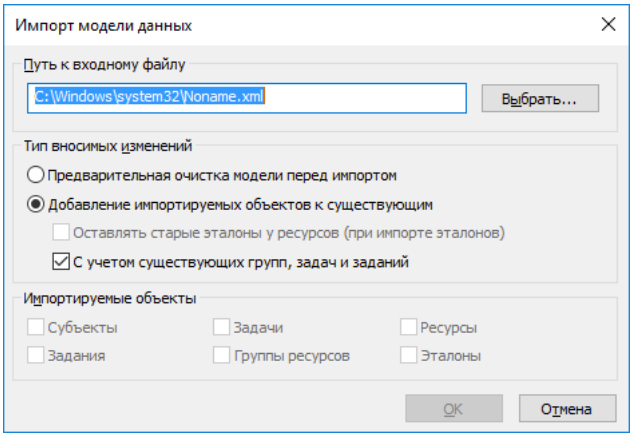
Импортом из файла с сохраненной моделью данных добавляются списки ресурсов, экспортированные из другой модели данных. Данный способ используется при переносе настроек защитных механизмов с одного компьютера на другой. Компьютеры должны иметь сходные конфигурации и использовать одинаковое программное обеспечение.

Примечание. Если централизованными средствами был создан файл, содержащий задачи со сценариями, то при импорте его в программу в локальном режиме будет запущено выполнение сценариев.

Для общего импорта в модель данных:

1. В меню "Файл" выберите команду "Импорт модели из XML".
2. Если с момента последнего сохранения модели в базе данных списки объектов были изменены, на экране появится сообщение, предупреждающее о потере изменений после загрузки модели. Нажмите кнопку "Да".

   На экране появится диалог настройки параметров импорта.



3. В поле "Путь к входному файлу" введите полное имя файла, в котором хранятся данные об объектах. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге открытия файла ОС Windows.
4. В группе полей "Тип вносимых изменений" выберите режим импорта. Для этого установите отметку в одном из следующих полей:

Поле	Пояснение
Предварительная очистка модели перед импортом	Перед импортом удаляются объекты текущей модели данных. После импорта модель будет состоять только из объектов, содержащихся в файле
Добавление импортируемых объектов к существующим	После импорта модель будет содержать как импортированные объекты, так и объекты текущей модели данных. При импорте возможна ситуация "дублирования" объектов. Это происходит, если отключен параметр "С учетом существующих групп, задач и заданий" или если в модели уже есть объекты этих категорий с такими же названиями. Если объекты относятся к категориям "Задания", "Задачи" или "Группы ресурсов", то после импорта модель данных будет содержать пары дублирующихся объектов. Добавляемый объект каждой пары будет иметь имя: имя_объекта<N>, где "N" — порядковый номер дублируемого объекта. Для объектов категории "Ресурсы" дублирующиеся объекты не создаются. При импорте ресурсов вместе с эталонными значениями можно выбрать режим сохранения эталонных значений дублирующихся ресурсов. Чтобы все эталонные значения были сохранены, установите отметку в поле "Оставлять старые эталоны у ресурсов (при импорте эталонов)". Иначе после импорта будут оставлены только те эталонные значения дублирующихся ресурсов, которые хранятся в файле

5. В группе полей "Импортируемые объекты" выберите категории объектов, которые следует импортировать. Для этого отметьте названия соответствующих категорий (если в выбранном файле нет данных об объектах какой-либо категории, соответствующее ей поле будет заблокировано).

Внимание! При выборе следует учитывать возможные связи объектов различных категорий. Импорт осуществляется только для объектов выбранных категорий, поэтому их связи с объектами других невыбранных категорий будут нарушены. Например, импортированные задания не будут включать задачи и группы ресурсов, если не выбраны категории "Задачи" и "Группы ресурсов".

6. Если выбрана категория "Ресурсы" и в файле хранятся сведения об эталонных значениях ресурсов, можно включить режим импорта ресурсов с эталонными значениями. Для этого установите отметку в поле "Эталоны".

Примечание. При включенном режиме импорта ресурсов вместе с эталонными значениями программе потребуется сохранить импортированную модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Эталоны".

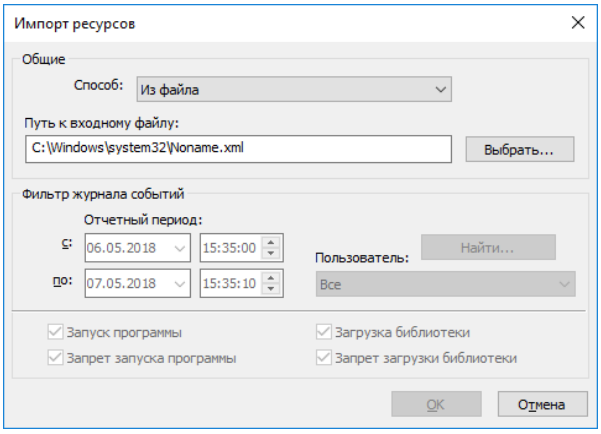
7. Нажмите кнопку "OK" в диалоге настройки параметров импорта.

Для импорта объектов текущей категории:

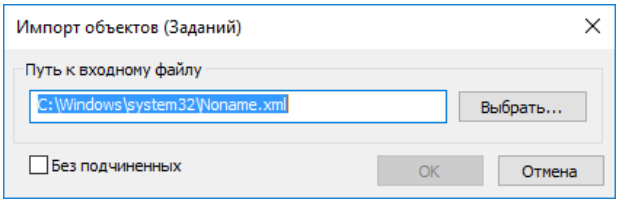
1. На панели категорий выберите категорию, в которую нужно импортировать объекты (кроме категории "Субъекты управления").
2. В окне структуры выберите корневой элемент. Откройте меню с названием элемента (например, "Задание") и выберите команду "Импорт и добавление".

   На экране появится диалог настройки параметров импорта.

   - Если выбрана категория "Ресурсы", диалог имеет вид:



   - Если выбрана категория "Задания", "Задачи" или "Группы ресурсов", диалог имеет вид:



3. В поле "Путь к входному файлу" введите полное имя файла, в котором хранятся данные об объектах. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге открытия файла ОС Windows.
4. По умолчанию совместно с объектами выбранной категории импортируются и связанные с ними цепочки объектов нижележащих уровней иерархии (например, группа ресурсов – ресурсы). Если требуется импортировать только объекты выбранной категории без включенных в них объектов, установите отметку в поле "Без подчиненных". (Данное поле отсутствует в диалоге настройки параметров импортирования для категории "Ресурсы".)
5. Нажмите кнопку "OK".

   Объекты, хранящиеся в файле, будут добавлены в список объектов текущей категории. При импорте возможны ситуации дублирования объектов, т. е. для импортируемых объектов имеются идентичные в текущей модели данных. Если такие объекты относятся к категориям "Задания", "Задачи" или "Группы ресурсов", после импорта модель данных будет содержать пары дублирующихся объектов. При этом один из объектов каждой пары переименовывается следующим образом: имя_ объекта<N>, где "N" — порядковый номер дублируемого объекта (например, "Группа ресурсов" и "Группа ресурсов1"). Для объектов категории "Ресурсы" дублирующиеся объекты не импортируются.

Примечание. Избирательный импорт эталонных значений ресурсов не осуществляется. Если требуется импортировать эталонные значения, выполните процедуру общего импорта модели данных (см. выше).

Внесение изменений в модель данных

На этапе создания модели данных, а также в процессе эксплуатации Secret Net Studio в модель можно вносить изменения. Необходимость изменений, как правило, обусловливается следующими факторами:

- появление новых задач по защите ресурсов;
- обновление программного обеспечения компьютера;
- изменения в задачах (расписание, методы контроля);
- полное или временное снятие задач с контроля.

Все операции, связанные с изменениями в модели данных, можно условно объединить в следующие группы:

Далее в данном разделе рассматриваются вопросы, связанные с особенностями перечисленных операций, и приводятся процедуры их выполнения.

Изменение параметров объектов

Каждый объект имеет свой набор параметров. Следует иметь в виду, что изменение значений некоторых параметров объектов может быть недоступно.

Ниже приведены параметры объектов каждой категории и даны пояснения по их применению.

Параметры ресурсов

Параметрами, определяющими свойства ресурса, являются:

- тип ресурса;
- имя и полный путь (кроме скриптов);
- признак "контролировать";
- эталоны;
- дополнительные параметры.

Значения параметров "тип" и "имя и путь" задаются при создании описания ресурса и изменению не подлежат.

Примечание. Путь может быть задан явно (абсолютный путь) или с помощью переменных окружения (см. стр.156).

Эталоном называется вычисленное контрольное значение для ресурса. Ресурс может входить в несколько заданий, и в каждом из них может использоваться свой метод контроля. Кроме того, в зависимости от типа ресурса и метода контроля могут использоваться разные алгоритмы. Поэтому ресурс может иметь несколько значений эталонов.

Признак "контролировать" означает, что после включения механизма контроля целостности (т. е. после связывания задания с компьютером) данный ресурс будет подлежать контролю. Отсутствие признака означает, что ресурс, даже если включен в задание КЦ, контролироваться не будет. Таким образом, устанавливая или удаляя признак, можно включать или отключать контроль конкретного ресурса.

Для исполняемых файлов процессов (файлы с расширением .exe, а также файлы, перечисленные в списке "Имена исполняемых модулей процессов" в параметрах программы управления КЦ-ЗПС — см.стр.280) можно настраивать следующие дополнительные параметры:

- параметры исключений, которые будут применяться во время действия механизма ЗПС — позволяют разрешить выполнение процессом любых скриптов (например, запускаемых в программе Internet Explorer) или файлов из определенных каталогов, включая вложенные каталоги. С помощью этой функции реализуется возможность запуска в жестком режиме ЗПС таких программ, как, например, Photoshop и SolidWorks;
- параметры изоляции процесса — позволяют обеспечить изолированную среду для процесса (запретить обмен данными с другими процессами).

Для изменения параметров ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог настройки параметров ресурса.
2. При необходимости измените состояние признака "Контролировать".
3. Для пересчета эталона выберите его в списке и нажмите кнопку "Пересчитать".

   Эталон будет пересчитан и в соответствующей ему строке в графе "Создан" появится новая запись о дате и времени пересчета.

4. Для расчета нового эталона и сохранения его предыдущего значения нажмите кнопку "Дубль-пересчет".

   Новый эталон будет пересчитан и сохранен вместе с предыдущим значением.

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

6. Если ресурс является исполняемым файлом, настройте дополнительные параметры исключений для механизма ЗПС и изоляции процесса. Для этого нажмите кнопку "Дополнительно" и в появившемся диалоге выполните следующие действия:
   - чтобы разрешить выполнение процессом любых скриптов, установите отметку в поле "Разрешить выполнять любые скрипты";
   - чтобы разрешить процессу запуск файлов из определенных каталогов, установите отметку в поле "Разрешить выполнять любые модули из указанных каталогов" и сформируйте список каталогов. Для добавления каталога в список введите путь к нему (путь можно ввести вручную или указать в стандартном диалоге, вызываемом с помощью кнопки справа от строки ввода) и нажмите кнопку добавления "+". Для удаления каталога из списка выберите этот каталог и нажмите кнопку удаления "-";
   - чтобы включить изоляцию процесса, установите отметку в поле "Изолировать процесс";
   - нажмите кнопку "ОК".

7. Нажмите кнопку "ОК" в диалоге настройки параметров ресурса.

Параметры группы ресурсов

Параметрами, определяющими свойства группы ресурсов, являются:

- имя группы;
- описание;
- тип ресурсов, входящих в данную группу.

Имя группы и краткое описание можно изменить в любой момент. Тип ресурсов можно изменить только в случае, если группа не содержит ни одного ресурса.

Для изменения параметров группы:

1. Выберите группу, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог с параметрами группы. В полях "Имя" и "Описание" изменения вносятся вручную, а в поле "Тип" значение выбирается из списка.

2. Внесите необходимые изменения и нажмите кнопку "ОК".

Параметры задачи

В свойствах задачи указываются имя, описание задачи и сценарий (при централизованном управлении). Задачи со сценарием обозначаются пиктограммой  .

Для изменения параметров задачи:

1. Выберите задачу, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог для настройки параметров задачи.

2. Если требуется внести изменения в сценарий, нажмите кнопку "Сценарий" (составление сценария описано на стр.**150**).

3. Внесите изменения в поля "Имя" и "Описание" и нажмите кнопку "ОК".

Параметры задания

Свойства задания КЦ определяются группой общих параметров и расписанием. В общую группу параметров входят:

- имя и описание задания;

- вид задания — тиражируемое/нетиражируемое (только для централизованного управления);
- методы и алгоритмы контроля;
- реакция системы на результаты контроля.

Методы и алгоритмы контроля, реакция системы и расписание — параметры, определяющие порядок КЦ ресурсов в рамках данного задания. При изменении методов и алгоритмов контроля необходимо учитывать типы ресурсов, связанных с заданием, так как к каждому типу ресурсов может применяться только определенный метод (или набор методов) КЦ. Кроме того, следует учитывать, что после изменения метода контроля может потребоваться корректировка реакции системы на результат проверки. Например, метод восстановления содержимого может применяться только с алгоритмом "полное совпадение".

Свойства задания ЗПС определяют следующие параметры:

- имя;
- краткое описание;
- вид (тиражируемое/нетиражируемое).

Для изменения параметров задания:

1. Выберите задание, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог для настройки параметров задания.

2. Настройте доступные для изменения параметры и нажмите кнопку "OK". Действия выполняются аналогично процедуре формирования задания (см. стр.**119**).

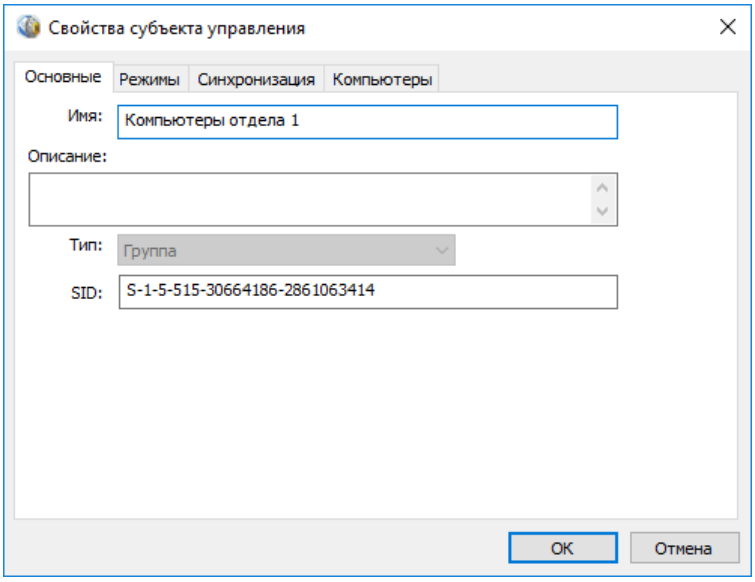
Параметры субъектов

Свойства субъекта управления определяют основные параметры (имя, тип и пр.), а также в зависимости от типа субъекта можно настраивать дополнительные параметры применения режимов, синхронизации данных и списки компьютеров для групп.

Для изменения параметров субъекта:

1. Выберите субъект, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалоговое окно, подобное представленному на рисунке:



   В зависимости от типа субъекта и режима работы программы могут быть представлены следующие диалоги:

   - "Основные" — содержит основные параметры субъекта (имя, описание, тип и идентификатор субъекта).

- "Режимы" — диалог представлен для компьютеров и групп компьютеров и содержит следующие параметры:
  - способ задания режима ЗПС (централизованно или локально);
  - состояние механизма ЗПС (включен или отключен);
  - режим работы механизма ЗПС (жесткий или мягкий);
  - режимы дополнительной проверки целостности модулей и их заголовков перед запуском и контроля выполнения сценариев (скриптов);
  - состояние режима изоляции процессов;
  - разрешение или запрет выполнения заданий КЦ и ЗПС, созданных в локальных моделях данных.
- "Синхронизация" — диалог представлен для компьютеров и групп компьютеров в централизованном режиме работы программы и содержит параметры синхронизации ЦБД и ЛБД.
- "Компьютеры" — диалог представлен для групп компьютеров и предназначен для просмотра и редактирования состава группы (возможность редактирования отсутствует для групп по умолчанию SecretNetICheckDefault).

2. Настройте доступные для изменения параметры и нажмите кнопку "ОК".

Добавление объектов

Следует иметь в виду, что само по себе добавление объектов не влечет за собой изменений в работе защитных механизмов. Для того чтобы изменения вступили в силу, добавленные объекты должны быть связаны с уже существующими объектами. Так, например, новый ресурс, добавленный в модель, необходимо включить в группу ресурсов. Группа ресурсов должна быть включена в задачу, а задача — в задание (также допускается включить группу ресурсов непосредственно в задание). Наконец, задание необходимо связать с одним из субъектов — компьютером, пользователем, группой пользователей или компьютеров.

Добавление ресурса

Добавить новые ресурсы в модель данных можно одним из следующих способов:

Способ	Пояснение
Автоматически в процессе генерации задач	Генерация задачи сопровождается автоматическим включением в нее всех связанных с ней ресурсов. Перед началом генерации можно задать дополнительное условие: включать или не включать объекты реестра и добавлять или не добавлять зависимые модули. Добавленные ресурсы связаны с объектом "Задача"
Вручную	Ресурсы выбираются из общего перечня ресурсов компьютера. Вручную можно добавить как одиночный ресурс (например, файл или ключ реестра), указав его явно, так и несколько ресурсов, удовлетворяющих задаваемому условию. Добавляемые ресурсы не связаны с другими объектами
Средствами импорта	Список ресурсов можно импортировать из следующих источников: • файл с сохраненной моделью данных (см. стр.**137**); • журнал безопасности ОС Windows или журнал Secret Net Studio на данном компьютере либо сохраненный журнал в файле (см. далее)
Добавлением ресурса в группу	Ресурс включается в одну из существующих групп. При этом ресурс может быть выбран как из списка уже включенных в модель, так и из общего списка всех ресурсов компьютера. Добавленный ресурс связан с объектом "Группа ресурсов"

Для добавления вручную одиночного ресурса:

1. Выберите категорию "Ресурсы" и выберите в меню команду "Ресурсы | Создать ресурс(ы) | Одиночный".

   На экране появится диалог для выбора назначения ресурса.
2. Выберите нужное назначение ресурса:
   - "Ресурс Windows" — если добавляется файл, каталог, переменная реестра или ключ реестра;
   - "Исполняемый ресурс" — для добавления исполняемого сценария (скрипта).
3. Нажмите кнопку "ОК".

   Появится диалог для настройки параметров ресурса.
4. Укажите параметры добавляемого ресурса (см. таблицу ниже) и нажмите кнопку "ОК".

   Для файла, каталога, переменной реестра или ключа реестра настраиваются следующие параметры:

Параметр	Пояснение
Тип	Укажите тип добавляемого ресурса: файл, каталог, переменная реестра, ключ реестра
Имя и путь	Введите вручную имя и полный путь к добавляемому ресурсу или нажмите кнопку "Обзор" и воспользуйтесь стандартной процедурой ОС
Контролировать	Отметка, установленная в этом поле, означает, что после включения механизма контроля целостности данный ресурс будет контролироваться. Если по каким-либо причинам контроль данного ресурса требуется отложить на неопределенное время, удалите отметку. В этом случае описание ресурса сохранится в модели данных и его можно будет поставить на контроль позднее
Выполняемый	Параметр доступен, если тип добавляемого ресурса — файл. Используется для обозначения исполняемых файлов, которые формируют списки программ, разрешенных для запуска при включенной замкнутой программной среде

   Для исполняемого сценария (скрипта) настраиваются следующие параметры:

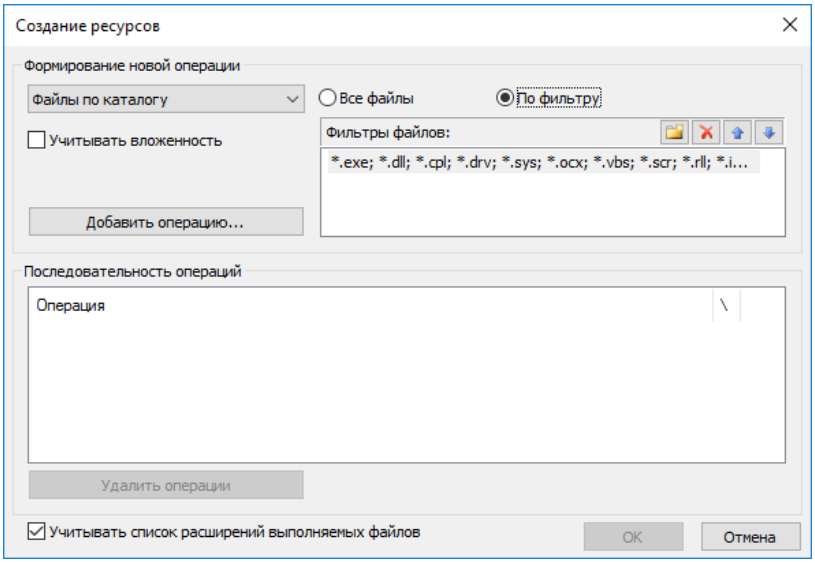
Параметр	Пояснение
Имя	Введите имя ресурса, уникальное для списка ресурсов. В качестве имени ресурса можно указать, например, имя файла, из которого загружен сценарий (скрипт)
Описание	Введите дополнительные сведения о ресурсе
Содержимое	Введите текст сценария (скрипта) — последовательность исполняемых команд и/или действий, обрабатываемых по технологии Active Scripts. Текст сценария можно ввести вручную или загрузить из файла с помощью кнопки "Загрузить…". Для загрузки текста могут использоваться файлы, содержащие сценарии с использованием технологии Active Scripts (например, vbs-файлы)

   Ресурс появится в списке основного окна программы. Далее с этим ресурсом можно выполнять все необходимые операции (добавить его в группу, включить в задачу и т. д.).

Для добавления вручную нескольких ресурсов:

1. Выберите категорию "Ресурсы" и выберите в меню команду "Ресурсы | Создать ресурс(ы) | Несколько".

   На экране появится диалог:



Диалог состоит из двух частей. Верхняя часть диалога (группа "Формирование новой операции") предназначена для указания варианта отбора ресурсов и задания дополнительных условий. Дополнительные условия задаются в зависимости от выбранного варианта. Одному варианту можно задать несколько условий для добавления ресурсов с использованием фильтров. Чтобы выполнить операцию, необходимо выбрать вариант, задать дополнительные условия и затем нажать кнопку "Добавить операцию".

Нижняя часть диалога (группа "Последовательность операций") предназначена для отображения последовательности выполненных операций.

Параметры, используемые при выполнении операции, описаны в приведенной ниже таблице.

Параметр	Пояснение
Вариант отбора ресурсов	Предусмотрены следующие варианты: • Выбранные файлы (стандартная процедура выбора файлов, дополнительные условия недоступны). • Файлы по каталогу (добавляются файлы, входящие в указанный каталог, учитывается вложенность, можно использовать фильтр). • Каталоги с файлами (учитывается вложенность, можно использовать фильтр). • Каталоги по каталогу (учитывается вложенность). • Переменные по ключу (выбираются переменные по ключу реестра, учитывается вложенность). • Ключи с переменными (выбираются ключи с переменными, учитывается вложенность)
Учитывать вложенность	Учитывается вложенность ресурсов для всех вариантов отбора, кроме варианта "Выбранные файлы"
Все файлы	Выбираются все ресурсы для вариантов "Файлы по каталогу" и "Каталоги с файлами"
По фильтру	Включение фильтра для вариантов "Файлы по каталогу" и "Каталоги с файлами". Если в списке имеется несколько фильтров, то для отбора файлов будет использоваться тот, который выбран в списке
Учитывать список расширений выполняемых файлов	Устанавливается признак "выполняемый" для файлов, которые имеют определенные расширения или имена, заданные параметрами "Расширения выполняемых" и "Имена исполняемых модулей процессов" в параметрах программы (см.стр.280). Файлы с этим признаком при отображении в окне программы управления КЦ-ЗПС отмечаются специальным значком

Настройка фильтров. При включении параметра "По фильтру" становится доступным список фильтров. Каждому фильтру соответствует одна строка, в которой указаны расширения файлов, добавляемых в модель данных. По умолчанию в списке содержится один фильтр, обеспечивающий отбор файлов с расширениями *.exe; *.dll; *.cpl; *.drv; *.sys; *.ocx; *.vbs; *.scr; *.rll; *.ime; *.bpl; *.ax; *.acm; *.com; *.ppl; *.cmd; *.bat. При необходимости его можно изменить или добавить в список новые фильтры. Расширения файлов в строке разделяются точкой с запятой, запятой или пробелом.

- Для изменения фильтра выберите строку, нажмите клавишу <F2> и отредактируйте список расширений файлов.
- Для добавления нового фильтра нажмите кнопку "Новый" и в появившейся строке введите список расширений файлов.
- Для удаления фильтра из списка выберите его и нажмите кнопку "Удалить".
- Для перемещения строки в списке выберите ее и нажмите кнопку со стрелкой.

2. Настройте параметры отбора ресурсов. Для этого выберите нужный вариант в раскрывающемся списке: "Выбранные файлы", "Файлы по каталогу", "Каталоги с файлами", "Каталоги по каталогу", "Переменные по ключу" или "Ключи с переменными".
3. Если выбран вариант "Выбранные файлы", нажмите кнопку "Добавить операцию". Для остальных вариантов — перейдите к выполнению действия **5**.

   Появится стандартный диалог ОС Windows для выбора файлов.
4. Выберите нужные файлы.

   В нижней части диалога появится список операций. Каждому выбранному файлу соответствует своя операция.

   Примечание. Если требуется удалить операции, выберите их в списке и нажмите кнопку "Удалить операции".

   Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
5. Если выбран вариант "Файлы по каталогу", "Каталоги с файлами" или "Каталоги по каталогу", настройте дополнительные параметры (при использовании фильтра выберите его в списке) и нажмите кнопку "Добавить операцию". Для остальных вариантов — перейдите к выполнению действия **7**.

   Появится стандартный диалог ОС Windows для выбора каталога.
6. Выберите каталог и нажмите кнопку "ОК".

   Диалог выбора каталога закроется и в нижней части диалога "Создание ресурсов" в список добавится описание выполненной операции.

   Примечание. Если требуется удалить операции, выберите их в списке и нажмите кнопку "Удалить операции".

   Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
7. Если выбран вариант "Переменные по ключу" или "Ключи с переменными", отметьте при необходимости поле "Учитывать вложенность" и нажмите кнопку "Добавить операцию".

   Появится стандартный диалог ОС Windows для просмотра реестра.
8. Выберите ключ реестра и нажмите кнопку "ОК".

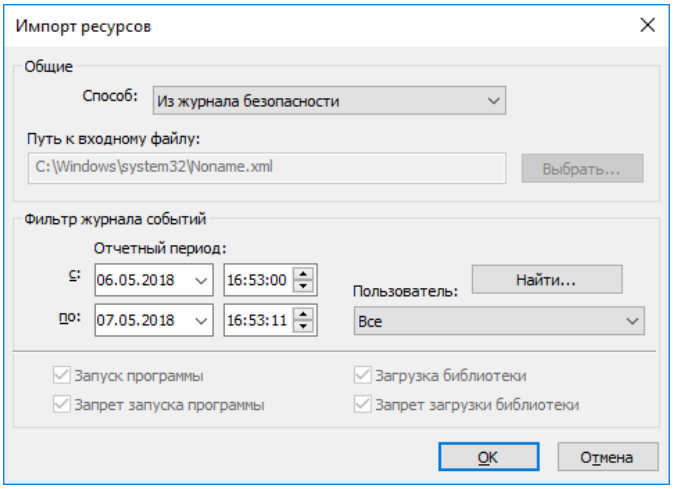
   Диалог просмотра реестра закроется и в нижней части диалога "Создание ресурсов" в список добавится описание выполненной операции.
9. Проверьте список выполненных операций и, если он содержит все ресурсы, которые планировалось включить в модель данных, нажмите кнопку "ОК".

   Диалог "Создание ресурсов" закроется, а выбранные ресурсы будут добавлены в модель данных.

Для импорта списка ресурсов из журнала безопасности ОС Windows:

1. Выберите категорию "Ресурсы" и затем выберите в меню команду "Ресурсы | Импорт и добавление".

   На экране появится диалог:



2. Выберите в списке поля "Способ" значение "Из журнала безопасности".

   Станут доступны настройки фильтра, по которым из журнала безопасности ОС Windows будут отбираться ресурсы. Настройки включают в себя отчетный период (дата и время) и имя пользователя.

3. Задайте отчетный период и укажите пользователя, по результатам работы которого будут отбираться ресурсы. При этом можно указать "Все" (в данном случае будут отбираться ресурсы, к которым обращались все пользователи) или выбрать отдельного пользователя.

   Для выбора пользователя выполните следующее:

   - Нажмите кнопку "Найти".

     Кнопка "Найти" исчезнет, начнется анализ журнала безопасности и, если в журнале были зарегистрированы обращения пользователей к ресурсам, эти пользователи будут внесены в раскрывающийся список.
   - Выберите нужного пользователя из раскрывающегося списка.

4. Нажмите кнопку "OK".

Для импорта списка ресурсов из журнала Secret Net Studio:

1. Выберите категорию "Ресурсы" и затем выберите в меню команду "Ресурсы | Импорт и добавление".

   На экране появится диалог (см. предыдущую процедуру).

2. Выберите в списке поля "Способ" значение "Из журнала Secret Net Studio".

   Станут доступными настройки фильтра, по которым из журнала Secret Net Studio будут отбираться ресурсы. Настройки включают в себя отчетный период (дата и время), имя пользователя и тип регистрируемого события.

   Примечание. Из журнала Secret Net Studio импортируется информация о ресурсах, связанных с событиями: запуск программы, запрет запуска программы, загрузка библиотеки и запрет загрузки библиотеки.

3. Настройте параметры фильтра и нажмите кнопку "OK".

   Примечание. По умолчанию импортируется информация о ресурсах, связанных со всеми предусмотренными событиями. Чтобы не импортировать ресурсы, связанные с определенным событием, удалите соответствующую отметку. Для выполнения процедуры необходимо, чтобы была установлена хотя бы одна отметка.

Для добавления ресурса в группу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в дополнительном окне структуры группу, в которую предполагается добавить новые ресурсы, вызовите контекстное меню и выберите команду "Добавить ресурсы", а затем команду:

   - "Существующие" — для выбора ресурсов из числа имеющихся в модели данных, но не входящих в данную группу.

- "Новый одиночный" — для добавления одиночного ресурса (описание процедуры добавления вручную одиночного ресурса см. выше).
- "Несколько новых" — для добавления нескольких ресурсов (описание процедуры добавления вручную нескольких ресурсов см. выше).
- "Импортировать" — для импорта списка ресурсов из другого источника: из файла (описание процедуры импорта объектов см. на стр.**139**), из журнала безопасности или журнала Secret Net Studio (описание процедур импорта ресурсов из журналов см. выше).

Выбранные ресурсы будут добавлены в группу.

Добавление группы ресурсов

Новую группу ресурсов можно добавить в модель данных:

- вручную;
- по каталогу;
- по ключу реестра;
- по журналу;
- средствами импорта.

Примечание. Следует иметь в виду, что вручную, по каталогу и по ключу реестра можно добавить группу ресурсов непосредственно в задачу. Добавленная таким способом группа ресурсов будет связана с вышестоящим объектом.

Источником при добавлении группы ресурсов по журналу в централизованном режиме является файл, в который предварительно были экспортированы сведения из журнала. В локальном режиме источником может быть журнал безопасности или журнал Secret Net Studio.

Для добавления группы ресурсов вручную:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | Вручную".

   Появится диалог для настройки параметров группы ресурсов.
3. Заполните поля диалога и нажмите кнопку "OK". Тип группы ресурсов (в поле "Тип") должен быть указан в соответствии с ее назначением.

   Новая группа будет добавлена в список групп ресурсов.

Для добавления группы ресурсов по каталогу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По каталогу".

   Появится стандартный диалог ОС Windows для выбора каталога.
3. Выберите каталог и нажмите кнопку "OK".

   Новая группа будет добавлена в список групп ресурсов, а файлы каталога — в список ресурсов данной группы.

Для добавления группы ресурсов по ключу реестра:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По ключу реестра".

   Появится стандартный диалог ОС Windows для просмотра реестра.
3. Выберите в соответствующем разделе нужный ключ реестра и нажмите кнопку "OK".

   Ресурсы, соответствующие выбранному ключу реестра, будут добавлены в составе новой группы в модель данных.

Для добавления группы ресурсов по журналу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По журналу".

На экране появится диалог для выбора типа ресурсов, которые будут определены по записям журнала — загружаемые модули приложений или исполняемые скрипты.

3. Выберите нужный тип ресурсов для получения из журнала:
   - "Загружаемые модули" — если группа должна содержать файлы, которые загружались при работе приложений;
   - "Исполняемые скрипты" — если группа должна содержать скрипты, о загрузке которых имеются сведения в журнале.
4. Нажмите кнопку "OK".

   На экране появится диалог настройки.
5. В централизованном режиме нажмите кнопку "Выбрать" и выберите файл, в который предварительно были экспортированы сведения из журнала (в формате snlog или dvt).

   В локальном режиме выберите способ (журнал безопасности или журнал Secret Net Studio).

   В зависимости от режима и выбранного способа станут доступными настройки фильтра журнала событий.
6. Настройте параметры фильтра и нажмите кнопку "OK".

   Появится сообщение о добавлении в модель нового объекта.

Для добавления группы ресурсов средствами импорта:

1. Выберите категорию "Группы ресурсов".
2. Выберите команду "Импорт и добавление" в меню "Группы ресурсов" или в контекстном меню, вызванном к папке "Группы ресурсов".

   Появится диалог настройки параметров импорта.
3. Выполните действия для импорта объектов категории (описание процедуры импорта см. на стр.**139**).

Добавление задач

Добавить новую задачу в модель данных можно одним из следующих способов:

- вручную;
- вручную со сценарием;
- с помощью генератора задач (см. стр.**117**);
- с помощью средств импорта (см. стр.**139**).

Для добавления задачи вручную:

1. Выберите категорию "Задачи" и выберите в меню команду "Задачи | Создать задачу | Вручную".

   Появится диалог для настройки параметров задачи.
2. Введите имя задачи, ее краткое описание и нажмите кнопку "OK".

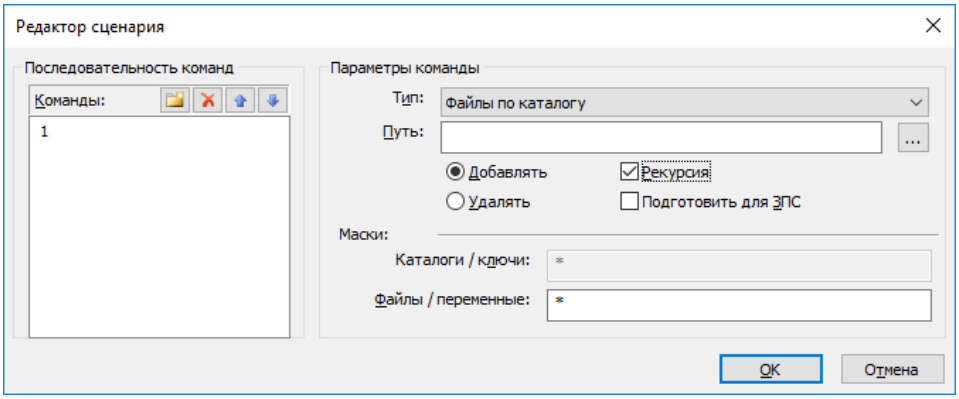
   В модели данных появится новая задача, не связанная с другими объектами.

Для добавления задачи со сценарием вручную:

1. Выберите категорию "Задачи" и выберите в меню команду "Задачи | Создать задачу | Вручную".

   Появится диалог для настройки параметров задачи.
2. Введите имя задачи и ее краткое описание.
3. Нажмите кнопку "Сценарий".

   Появится диалог:



Сценарий для задачи — это последовательность настраиваемых команд, определяющих правила отбора ресурсов в задачу.

4. Для добавления команды нажмите кнопку в левой части диалога и введите имя команды, отображающее ее смысловое содержание.

   В правой части диалога станут доступными поля для настройки параметров команды.

5. Выберите тип ресурсов и укажите путь.

   Предусмотренные типы перечислены в следующей таблице.

Тип ресурсов	Пояснение
Файлы по каталогу	Отбираются файлы из каталога, указанного в поле "Путь". Для отбора файлов можно использовать маску, заданную в поле "Файлы/Переменные"
Каталоги с файлами	Отбираются каталоги и файлы по указанному пути. При отборе можно использовать маски для каталогов и для файлов, заданные в полях группы "Маски"
Переменные по ключу	Отбираются только переменные реестра по заданному ключу реестра. Для задания базового ключа реестра указывается путь. При отборе можно использовать маску, заданную в поле "Файлы/Переменные"
Ключи с переменными	Отбираются переменные реестра по заданному ключу реестра и ключи. Для задания базового ключа реестра указывается путь. При отборе можно использовать маски, заданные в полях группы "Маски"
Установленные программы (MSI)	Отбираются ресурсы программы, выбранной в списке установленных программ (Microsoft Installer). Для отбора каталогов и файлов можно использовать маски, заданные в полях группы "Маски"
Компоненты Secret Net Studio	Отбираются ресурсы из состава ПО клиента системы Secret Net Studio
Файлы из переменных в указанном ключе реестра	Отбираются файлы, полученные из переменных реестра по заданному ключу реестра. Для задания базового ключа реестра указывается путь (например: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). При отборе можно использовать маску, заданную в поле "Файлы/Переменные"
Загружаемые драйверы и сервисы Windows	Отбираются файлы драйверов и служб операционной системы

В зависимости от выбранного типа некоторые поля для ввода параметров могут быть недоступны.

При выборе "Установленные программы MSI" поле "Путь" изменится на "Имя", а поле "Рекурсия" — на "Игнорировать объекты реестра".

6. Укажите действия для команды.

   Параметр "Добавлять" используется для добавления отбираемых ресурсов в общий список ресурсов задачи. Параметр "Удалять" — для удаления ресурсов из общего списка, сформированного предыдущими командами.

7. Для применения команды ко всем вложенным ресурсам поставьте отметку в поле "Рекурсия".

8. Если выбран тип "Файлы по каталогу" или "Каталоги с файлами", при необходимости используйте возможность добавления в список зависимых модулей (см. стр.**156**). Для добавления зависимых модулей установите отметку в поле "Подготовить для ЗПС". В этом случае автоматически будут также выбраны все зависимые модули для файлов, указанных с помощью маски. Они будут добавлены в модель и помечены как исполняемые. То есть результат будет таким же, как при выполнении процедуры поиска и добавления зависимых модулей, но не на данном компьютере, а на всех, где будет выполнен создаваемый сценарий.

9. В зависимости от выбранного типа ресурсов введите маску отбора ресурсов в поле "Каталоги/ключи" или "Файлы/переменные".

   В поле можно ввести несколько масок, разделяя их символами "," (запятая), ";" (точка с запятой) или пробел. По умолчанию устанавливается маска вида "*". Это означает, что будут отобраны все ресурсы, удовлетворяющие параметрам команды. Если удалить маску "*" и оставить поле пустым, команда выполнена не будет.

   Примечание. Для типа ресурсов "Установленные программы (MSI)" маску можно задать непосредственно в поле "Имя". При этом можно использовать любой из следующих способов задания маски: <фрагмент текста>*, *<фрагмент текста> или *<фрагмент текста>*.

10. Для добавления и настройки следующей команды повторите действия **4–9**.

    Для изменения последовательности выполнения команд используйте соответствующие кнопки в левой части диалога.

11. Нажмите кнопку "ОК". Затем нажмите кнопку "ОК" в диалоге свойств задачи.

    В основном окне программы появится задача с пиктограммой  .

Добавление заданий

Процедуры добавления задания подробно описаны на стр.**119**.

Добавление субъектов

В централизованном режиме в модель данных можно добавлять компьютеры и группы, включающие в себя компьютеры. В локальном режиме добавляются пользователи и группы пользователей. После добавления субъекты отмечены в списке знаком (как не связанные с другими объектами).

Для добавления компьютеров (централизованный режим):

1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".

   Появится диалог для выбора типа добавляемых субъектов.
3. Установите отметку в поле "Компьютер" и нажмите кнопку "ОК".

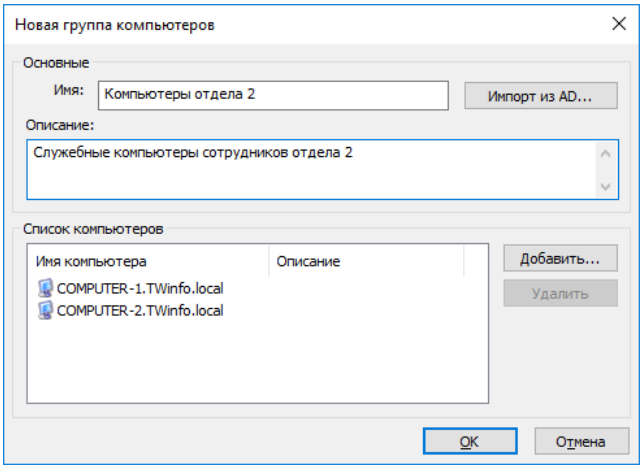
   Появится диалог со списком компьютеров домена безопасности с установленным клиентским ПО Secret Net Studio.
4. Выберите в списке нужные компьютеры и нажмите кнопку "ОК".

Для добавления группы компьютеров (централизованный режим):

1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".

   Появится диалог для выбора типа добавляемых субъектов.
3. Установите отметку в поле "Группа компьютеров" и нажмите кнопку "ОК".

   Появится диалог для настройки создаваемой группы.



4. Если в Active Directory имеется группа, которая содержит нужные компьютеры для создания группы в модели данных, можно импортировать из AD сведения об этом объекте. Для этого нажмите кнопку "Импорт из AD" и выберите нужную группу компьютеров в появившемся диалоге ОС Windows.
5. Введите имя и дополнительные сведения о создаваемой группе в соответствующих полях.
6. Сформируйте список компьютеров группы. Для добавления и удаления элементов списка используйте кнопки справа.
7. Нажмите кнопку "OK".

Для добавления пользователей и групп пользователей (локальный режим):

1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".

   Появится диалог ОС Windows для выбора пользователей и групп.
3. Найдите и выберите нужные объекты и нажмите кнопку "OK".

Удаление объектов

При удалении объекта из модели данных необходимо учитывать его связи с другими вышестоящими или подчиненными объектами. Так, перед удалением ресурса необходимо выяснить, в каких заданиях данный ресурс контролируется, и проанализировать возможные последствия его удаления.

Внимание! После удаления ресурсов из задания следует выполнить перерасчет эталонов.

Предупреждение. В локальном режиме из модели данных нельзя удалить субъект "Компьютер" и задания, задачи, группы ресурсов и ресурсы, добавленные в модель средствами централизованного управления. Также нельзя разорвать связи между такими объектами.

В централизованном режиме нельзя удалить группу по умолчанию SecretNetICheckDefault или SecretNetICheckDefault64 (в зависимости от разрядности ОС).

Для удаления объекта:

1. Найдите удаляемый объект, вызовите контекстное меню объекта и выберите команду "Удалить".

   Если в настройках программы отключено подтверждение удаления объектов, объект будет удален из модели данных. При этом будут удалены все подчиненные объекты, не имеющие связей с другими вышестоящими объектами, и на этом процедура удаления завершится.

2. Если в настройках программы включено подтверждение при удалении объектов, появится диалог, отображающий связи удаляемого объекта с вышестоящими и подчиненными объектами. При необходимости удалить из модели данных также подчиненные объекты поставьте отметку в поле "Удалять подчиненные". В этом случае будут удалены все подчиненные объекты, не имеющие связей с другими вышестоящими объектами.
3. Нажмите кнопку "Да".

   Объект будет удален из модели данных.

Для удаления всех объектов категории:

1. Выберите нужную категорию ("Субъекты управления", "Задания", "Задачи" или "Группы ресурсов"), в окне структуры вызовите контекстное меню для корневой папки и выберите команду "Удалить все".

   Появится диалог, отображающий связи объектов.
2. Если требуется удалить все подчиненные объекты, поставьте отметку в поле "Удалять подчиненные". Нажмите кнопку "Да".

   Все объекты, входящие в выбранную категорию, будут удалены из модели данных.

Связи между объектами

В зависимости от способа добавления новых объектов в модель соответствующие связи могут устанавливаться автоматически. Например, при добавлении в группу нового ресурса в модели устанавливается связь ресурс—группа. Связь может быть установлена также при импорте объекта.

В других случаях в модель добавляются объекты, не связанные с другими объектами, например, при создании вручную новой задачи или задания. Поэтому после добавления недостающие связи должны быть установлены вручную связыванием вышестоящего и подчиненного объекта.

Внимание! В локальном режиме в объекты, созданные централизованными средствами, нельзя добавить: в задание — задачу, в задачу — группу ресурсов, а в группу — ресурс.

Для связывания объектов:

1. Выберите категорию объекта, вызовите контекстное меню нужного объекта и выберите команду "Добавить <название объекта> | Существующие".

   На экране появится диалог со списком объектов, которые еще не связаны с данным объектом.
2. Выберите в списке нужные объекты и нажмите кнопку "ОК".

   В результате будет установлена связь между выбранными объектами и вышестоящим объектом.

Для удаления связи между объектами:

1. Выберите категорию объекта, у которого должна быть удалена связь с вышестоящим объектом, найдите объект, вызовите для него контекстное меню и выберите команду "Исключить из | <название объекта>".

   Примечание. Следует иметь в виду, что объект можно исключить одновременно из всех объектов вышестоящей категории.

   Появится предупреждение об удалении связей с вышестоящими объектами и предложение продолжить процедуру.
2. Нажмите кнопку "Да".

Новый расчет и замена эталонов

При внесении изменений в модель данных новый расчет эталонов контролируемых ресурсов можно выполнить так же, как и при настройке модели данных (см. стр.**126**). Кроме того, предусмотрены следующие способы:

- расчет эталонов отдельного ресурса;

- расчет эталонов нескольких произвольно выбранных ресурсов.

Расчет эталонов для ресурса выполняется по всем заданиям, в которые входит данный ресурс. Так как один и тот же ресурс может входить в разные задания и в каждом из заданий для него предусмотрен свой метод контроля, расчет эталонов выполняется для каждого метода.

При перерасчете эталонов может возникнуть необходимость сохранения прежних ("старых") значений. Например, при контроле содержимого файлов, изменяемых при автоматическом обновлении ПО.

Примечание. Если для контроля содержимого используется алгоритм "встроенная ЭЦП", сохранение предыдущих эталонов для данного алгоритма в большинстве случаев не требуется. Обычно после обновления ПО сертификаты подписанных файлов остаются неизменными, благодаря чему эталоны для этих файлов будут действительны как до обновления ПО, так и после.

Предыдущие ("старые") эталоны удаляются из локальной базы данных автоматически при каждом успешном завершении задания КЦ. При необходимости можно использовать команду немедленного удаления старых эталонов.

Для пересчета эталона отдельного ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и выберите команду "Свойства".

   Появится диалог "Свойства ресурса" (см. стр.**141**).
2. Выберите в списке эталон и нажмите кнопку "Пересчитать".

   Эталон будет пересчитан, и в его строке обновится дата расчета.
3. Выполните пересчет для остальных эталонов списка и нажмите кнопку "ОК".

Для расчета эталонов выбранных ресурсов:

1. Выберите категорию "Ресурсы" или разверните структуру модели таким образом, чтобы в окне списка объектов отображались ресурсы.
2. Выделите в списке ресурс или несколько ресурсов, вызовите контекстное меню и выберите команду "Расчет эталонов".

   На экране появится диалог "Расчет эталонов".
3. Выполните действия, описанные в процедуре расчета эталонов в локальном режиме, начиная с шага **2** (см. стр.**126**).

Для удаления старых эталонов:

- Выберите в меню команду "Сервис | Эталоны | Удаление старых".

  Старые эталоны будут удалены из модели данных.

Запрет использования локальных заданий

По умолчанию на компьютерах разрешается выполнение и локальных, и централизованных заданий. При необходимости можно отключить выполнение локальных заданий (созданных в ЛБД в локальном режиме работы программы), чтобы на компьютерах выполнялись только централизованные задания.

Отключение локальных заданий можно выполнить в свойствах нужного субъекта в централизованном режиме работы. Параметры могут быть заданы как для отдельных компьютеров, так и для групп компьютеров. При этом приоритет имеют отключенные параметры. Например, если для группы отключен параметр "Локальные задания ЗПС", такие задания будут запрещены на компьютере, даже если тот же параметр включен для самого компьютера.

Для отключения локальных заданий:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. Удалите отметки в соответствующих полях:

- чтобы отключить задания контроля целостности — удалите отметку из поля "Локальные задания КЦ";
- чтобы отключить задания замкнутой программной среды — удалите отметку из поля "Локальные задания ЗПС".

4. Нажмите кнопку "ОК".

Поиск зависимых модулей

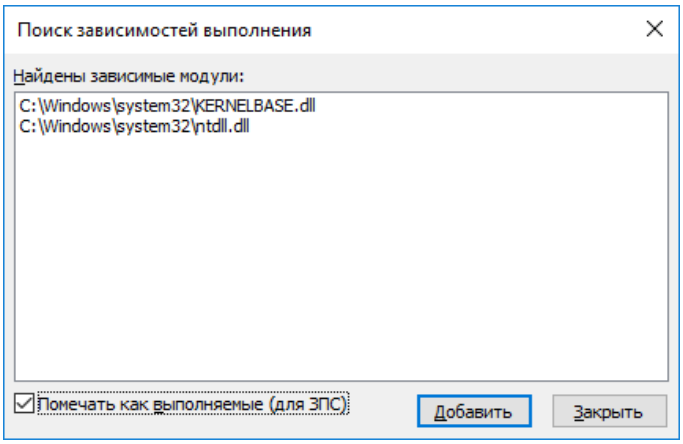
При работе пользователя с приложениями запуск исполняемых файлов может сопровождаться запуском модулей (драйверов и библиотек), не входящих непосредственно в приложения. Такие модули называются зависимыми.

При построении модели данных с помощью автоматизированных средств (мастера и механизма генерации задач) поиск зависимых модулей и добавление их в модель данных выполняются по умолчанию. При построении модели вручную и добавлении в нее новых ресурсов поиск зависимых модулей выполняется как отдельная процедура (см. ниже).

Для поиска и добавления зависимых модулей:

1. Выберите в области списка объектов ресурс или несколько ресурсов, вызовите контекстное меню и выберите команду "Зависимости".

   Появится диалог, содержащий список найденных зависимых модулей.



2. Чтобы зависимые модули не отмечались в модели данных как выполняемые, удалите отметку из поля "Помечать как выполняемые (для ЗПС)".
3. Нажмите кнопку "Добавить".

Модули будут добавлены в модель данных, затем появится сообщение об успешном завершении процедуры.

Замена переменных окружения

Для корректной работы модели данных, перенесенной с одного компьютера на другой, а также при экспорте отдельных ресурсов, задач и заданий может потребоваться заменить абсолютные пути к ресурсам на переменные окружения.

Данная процедура выполняется на том компьютере, с которого будет осуществляться перенос модели или экспорт ее отдельных элементов.

Замена переменных окружения на абсолютные пути — обратная операция, выполняемая в тех случаях, когда по каким-либо причинам необходимо восстановить абсолютные пути.

Для замены переменных окружения:

1. Выберите ресурс в модели данных и в контекстном меню выберите команду "Переменные окружения".

   Появится диалог, содержащий список имеющихся на компьютере переменных окружения.

2. Укажите направление замены:

- Для замены абсолютных путей на переменные окружения оставьте установленную по умолчанию отметку в переключателе.
- Для замены переменных окружения на абсолютные пути поставьте отметку в поле "Имена переменных окружения на значение путей в файлах и папках".

3. Выберите в списке те переменные, для которых будет выполнено действие.
4. Нажмите кнопку "ОК".

Настройка задания для ПАК "Соболь"

Задание для ПАК "Соболь" представляет собой перечень файлов жесткого диска и объектов системного реестра, целостность которых должна контролироваться средствами ПАК "Соболь" до загрузки ОС.

Внимание!

- Дополнительно комплекс "Соболь" может обеспечивать контроль целостности физических секторов жесткого диска, PCI-устройств и структур SMBIOS. Задание на контроль целостности указанных объектов формируется с помощью вспомогательного ПО комплекса "Соболь" (см. документацию на изделие).
- Задание на контроль целостности файлов и объектов реестра формируется средствами программы "Контроль программ и данных" из состава ПО системы Secret Net Studio.
- При совместном функционировании Secret Net Studio и комплекса "Соболь" в отношении объектов КЦ комплекса "Соболь" для локальных администраторов ОС устанавливается мягкий режим контроля целостности, а для всех остальных пользователей компьютера – жесткий. В мягком режиме при ошибке механизма контроля целостности вход в систему разрешается. В жестком режиме в аналогичной ситуации компьютер блокируется для входа всех пользователей, кроме администратора. В обоих режимах в журнале фиксируется событие об ошибке при контроле целостности.

После формирования модели данных с помощью мастера в ней появляется задание на контроль целостности ПАК "Соболь" (при включенном режиме интеграции).

Для настройки задания:

1. В главном окне программы "Контроль программ и данных" выберите категорию "Задания".
2. Добавьте в задание "Задание для ПАК "Соболь" все задачи контроля файлов средствами комплекса "Соболь".

   Примечание. Для добавления задач используйте описанные выше процедуры модификации модели данных.

3. При централизованном управлении установите связь этого задания со всеми компьютерами или группами, к которым это задание относится.
4. Для сохранения модели данных в базе данных Secret Net Studio выберите команду "Сохранить" в меню "Файл".
5. В меню "Сервис" выберите команду "Эталоны | Расчет".

   После расчета эталонов на экране появится сообщение: "Завершение процедуры расчета эталонов будет произведено ПАК "Соболь" при перезагрузке".
6. Нажмите кнопку "ОК".

Внимание! Если до начала выполнения данной процедуры в ПАК "Соболь" хранились собственные шаблоны контроля целостности файлов жесткого диска и объектов системного реестра, они будут заменены новыми, сформированными в соответствии с настройкой задания в программе "Контроль программ и данных".

При удалении всех задач из задания для ПАК "Соболь" или отключении режима интеграции собственные шаблоны ПАК "Соболь" будут восстановлены.

Глава 11
Полномочное управление доступом

Общие сведения о полномочном разграничении доступа

Механизм полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам. Ресурс считается конфиденциальным, если ему назначена категория конфиденциальности, отличная от категории для общедоступной информации (по умолчанию — "неконфиденциально"). Категорию можно назначить для следующих ресурсов:

- локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;
- каталоги и файлы на локальных физических дисках.

Пояснение. Каталогам и файлам, находящимся на устройствах из групп USB, PCMCIA, IEEE1394, Secure Digital (сменные носители), категория конфиденциальности непосредственно не назначается. Для них действует категория конфиденциальности, назначенная устройству.

Для сетевых интерфейсов можно указать уровни конфиденциальности сессий, в которых разрешается функционирование этих интерфейсов (используется в режиме контроля потоков).

Для принтеров можно указать категории конфиденциальности документов, разрешенных для печати.

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска.

Категории конфиденциальности ресурсов

Категория конфиденциальности является атрибутом ресурса. По умолчанию в механизме полномочного управления доступом используются следующие категории конфиденциальности:

- "неконфиденциально";
- "конфиденциально";
- "строго конфиденциально".

При необходимости можно увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации. Максимально возможное количество категорий — 16.

После установки клиентского ПО системы Secret Net Studio всем каталогам и файлам на локальных дисках компьютера назначена категория "неконфиденциально" (если ресурсы не имеют ранее присвоенных категорий конфиденциальности). Повышение категорий конфиденциальности нужных файлов осуществляется пользователями в пределах своих уровней допуска. При этом понижать категории конфиденциальности ресурсов, а также повышать категории каталогов разрешено только пользователям, которым предоставлена привилегия на управление категориями конфиденциальности.

Для устройств, которым можно назначить категорию конфиденциальности или выбрать допустимые уровни конфиденциальности сессий, по умолчанию включен режим доступа "без учета категории конфиденциальности" или "адаптер доступен всегда". Для принтеров по умолчанию включен режим разрешения печати документов любой категории конфиденциальности. Эти режимы разрешают использование устройств и принтеров независимо от уровня допуска пользователя. Назначение устройствам и принтерам категорий или уровней конфиденциальности выполняет администратор.

Наследование категорий конфиденциальности

В механизме полномочного управления доступом используется принцип наследования категорий конфиденциальности. Методы наследования различаются в зависимости от типов ресурсов.

Устройства наследуют категорию конфиденциальности от классов, к которым они относятся. При этом для класса разрешено указывать только категорию для общедоступной информации (по умолчанию — "неконфиденциально") или включить режим доступа "без учета категории конфиденциальности". За счет этого исключается возможность копирования конфиденциальной информации на неразрешенное подключенное устройство (при работе механизма в режиме контроля потоков и отсутствии у пользователя привилегии на вывод конфиденциальной информации).

В соответствии с правилами наследования при управлении устройствами (см. стр. **81**) явно заданные параметры имеют приоритет перед наследуемыми параметрами старших элементов иерархии. Поэтому если для устройства явно назначена категория конфиденциальности, она действует независимо от того, какая категория указана для класса.

Назначение категорий конфиденциальности для устройств и классов выполняется администратором при работе со списком устройств групповой политики.

Категория конфиденциальности локального физического диска имеет более высокий приоритет, чем категории файлов и каталогов, расположенных на этом устройстве. Если категория файла (каталога) ниже категории конфиденциальности устройства, система считает категорию файла (каталога) равной категории устройства. Если же категория файла (каталога) превышает категорию конфиденциальности устройства, такое состояние считается некорректным, и доступ к файлу (каталогу) запрещается.

На локальных физических дисках для объектов файловой системы из каталогов с категорией, отличной от категории для общедоступной информации (по умолчанию — "неконфиденциально"), действует принцип наследования. Наследование категории конфиденциальности объектами внутри каталога происходит в соответствии с признаками наследования, установленными в атрибутах этого каталога.

На локальных физических дисках назначение новым подкаталогам и файлам категории конфиденциальности каталога может выполняться автоматически путем наследования категории родительского каталога. Автоматическое назначение осуществляется, если для каталога включены режимы "Автоматически присваивать новым каталогам", "Автоматически присваивать новым файлам". При этом возможность изменения признаков доступна пользователю с привилегией на управление категориями конфиденциальности.

На всех подключенных к компьютеру устройствах из групп устройств USB, PCMCIA, IEEE1394, SD (сменные носители) самим файлам и каталогам категория конфиденциальности не назначается. Для всех этих файлов и каталогов всегда действует категория, назначенная устройству.

Уровни допуска и привилегии пользователей

Уровни допуска

Доступ пользователя к конфиденциальной информации осуществляется, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов (см. выше).

Пользователю разрешается доступ, если уровень допуска пользователя не ниже категории конфиденциальности ресурса. Например, пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями "конфиденциально" и "неконфиденциально", но запрещено открывать файлы с категорией "строго конфиденциально". Наивысший уровень допуска предоставляет возможность открывать файлы с любой категорией конфиденциальности.

По умолчанию всем пользователям назначен уровень допуска "неконфиденциально". Описание процедуры назначения уровня допуска см. на стр.**163**.

Привилегии пользователей

В механизме полномочного управления доступом используются привилегии, перечисленные в таблице ниже.

Привилегия	Описание
Управление категориями конфиденциальности	Пользователь может: • изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; • управлять режимом наследования категорий конфиденциальности каталогов (см. стр.**164**)
Печать конфиденциальных документов	Используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном механизме контроля печати
Вывод конфиденциальной информации	Пользователю разрешается выводить конфиденциальную информацию на внешние носители при включенном режиме контроля потоков. Внешними носителями в системе Secret Net Studio считаются сменные диски, для которых включен режим доступа "без учета категории конфиденциальности"

Привилегии предоставляются администратором безопасности пользователям, уполномоченным управлять конфиденциальностью ресурсов, распечатывать и копировать конфиденциальную информацию (см. стр.**163**). По умолчанию пользователям привилегии не предоставлены.

Режим контроля потоков механизма полномочного управления доступом

Режим контроля потоков конфиденциальной информации обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации. По умолчанию режим отключен. Для корректной работы системы перед включением режима необходимо выполнить дополнительную настройку. Основные действия для настройки выполняются локально с помощью специальной программы из состава клиентского ПО Secret Net Studio.

Уровень конфиденциальности сессии

При включенном режиме контроля потоков возможность использования устройств и доступа к конфиденциальным файлам определяется уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему. Уровень сессии не может быть выше уровня допуска пользователя. Сессия заканчивается вместе с сеансом работы пользователя на компьютере. Уровень сессии нельзя изменить до ее окончания.

При выполнении операций с ресурсами категории конфиденциальности ресурсов сравниваются с уровнем сессии. Доступ разрешается, если категория конфиденциальности ресурса ниже или совпадает с уровнем сессии. Запрещается доступ к ресурсам с более высокой категорией. Для всех создаваемых, скопированных или измененных документов присваивается категория конфиденциальности, равная уровню сессии.

Например, пользователь при входе в систему может выбрать уровень конфиденциальности сессии "конфиденциально" и тем самым запретить доступ к строго конфиденциальным ресурсам, даже если у него есть нужный уровень допуска. Однако следует иметь в виду, что неконфиденциальные документы, с которыми выполняются операции копирования и сохранения в конфиденциальной сессии, после выполнения операции станут конфиденциальными.

Из-за особенностей работы в конфиденциальных сессиях все действия, связанные с изменением конфигурации системы, необходимо выполнять в неконфиденциальной сессии или при отключенном режиме контроля потоков. В частности, конфиденциальную сессию нельзя использовать для настройки программного обеспечения, изменения режимов, а также для выполнения первичного входа пользователя на компьютер (когда формируется профиль учетной записи). Уровень конфиденциальности сессии, отличный от неконфиденциального, нужно выбирать только при работе с конфиденциальными данными.

Примечание. При использовании учетной записи Microsoft в ОС Windows 10 версии 2004 и включенном контроле потоков выбор уровня конфиденциальности сессии доступен только на компьютерах, включенных в домен.

Назначение сессии уровня конфиденциальности

В зависимости от заданных параметров присвоение сессии определенного уровня конфиденциальности может выполняться по выбору пользователя или автоматически системой. Автоматическое назначение уровня выполняется в следующих случаях:

- При включенном параметре "строгий контроль терминальных подключений". Параметр определяет условие для уровня конфиденциальности терминальной сессии при терминальном входе — этот уровень должен быть равен уровню конфиденциальности локальной сессии на терминальном клиенте (соответственно, режим контроля потоков в этом случае также должен быть включен на клиенте).
- При включенном параметре "автоматический выбор максимального уровня сессии". Если параметр включен, уровень конфиденциальности сессии принудительно устанавливается равным уровню допуска пользователя.

Использование устройств и сетевых интерфейсов

В режиме контроля потоков запрещается использование устройств, которым назначена категория конфиденциальности, отличающаяся от уровня сессии. Если на момент входа пользователя к компьютеру подключены устройства с различными категориями конфиденциальности, вход запрещается по причине конфликта подключенных устройств. Также запрещается вход в систему, если категория конфиденциальности подключенных устройств выше или ниже уровня допуска пользователя.

Режим контроля потоков позволяет установить ограничения на использование сетевых интерфейсов. Для каждого сетевого интерфейса можно указать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователю. Если открыта сессия с уровнем конфиденциальности, который не входит в список разрешенных уровней для сетевого интерфейса, его функционирование блокируется системой защиты.

Настройка полномочного разграничения доступа

Общий порядок настройки

Для использования на компьютерах механизма полномочного управления доступом выполните настройку в следующем порядке:

1. Задайте количество и названия категорий конфиденциальности (см. ниже).
2. Назначьте пользователям уровни допуска и привилегии (см. стр.**163**).

3. Присвойте ресурсам категории конфиденциальности (см. стр.**164**).
4. Настройте перечень регистрируемых событий (см. стр.**165**).
5. Для добавления маркеров в распечатываемые документы настройте и включите режим маркировки (см. стр.**105**).
6. Для ограничения вывода конфиденциальных документов на печать настройте использование принтеров (см. стр.**165**).
7. При необходимости включите режим скрытия конфиденциальных файлов (см. стр.**166**).
8. Для использования режима контроля потоков настройте и включите режим (см. стр.**166**).

В документе с комментариями к выпущенной версии (Release Notes) приведены последние актуальные рекомендации разработчиков по настройке механизма для работы с приложениями.

Перед началом использования механизма разъясните пользователям правила работы с конфиденциальными ресурсами.

Настройка категорий конфиденциальности

Внимание! Во избежание конфликтов в названиях категорий конфиденциальности для компьютеров с клиентом в сетевом режиме функционирования количество и названия категорий должны быть заданы в одной общей групповой политике, применяемой на компьютерах. В Центре управления рекомендуется настроить одну из следующих групповых политик (перечислены в порядке возрастания приоритета применения параметров):

- политика домена — для всех компьютеров, входящих в домен;
- политика организационного подразделения — для всех компьютеров, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности, — применяется на всех компьютерах, подчиненных этому серверу безопасности.

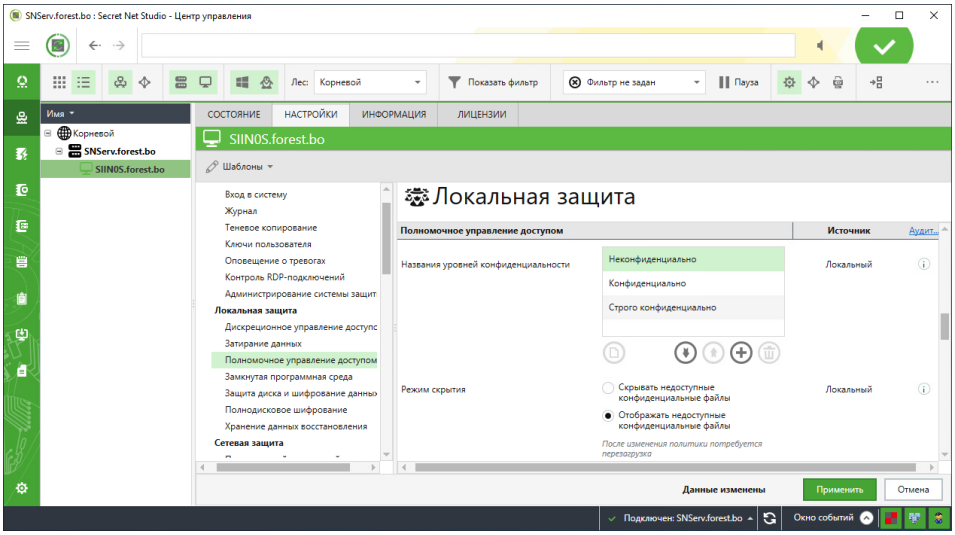
Например, все компьютеры, на которых будет обрабатываться конфиденциальная информация, можно включить в отдельное организационное подразделение и настроить категории в политике для этого подразделения.

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки количества и названий категорий конфиденциальности:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полномочное управление доступом".

   Пример содержимого группы параметров представлен на рисунке ниже.



3. Для параметра "Названия уровней конфиденциальности" сформируйте список категорий конфиденциальности. Для добавления, удаления или перемещения элементов используйте соответствующие кнопки под списком. Чтобы переименовать категорию, наведите на нее указатель и дважды нажмите левую кнопку мыши. При необходимости восстановить исходный набор категорий нажмите кнопку "По умолчанию".

   Примечание. Список упорядочен по степени важности категорий с точки зрения конфиденциальности информации. Наименьший уровень (приоритет) имеет первый элемент списка, наибольший уровень — у последнего элемента. Новые категории помещаются в конец списка, после чего их можно переместить на нужную позицию. Возможность удаления доступна для всех категорий, кроме первых трех элементов списка.

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

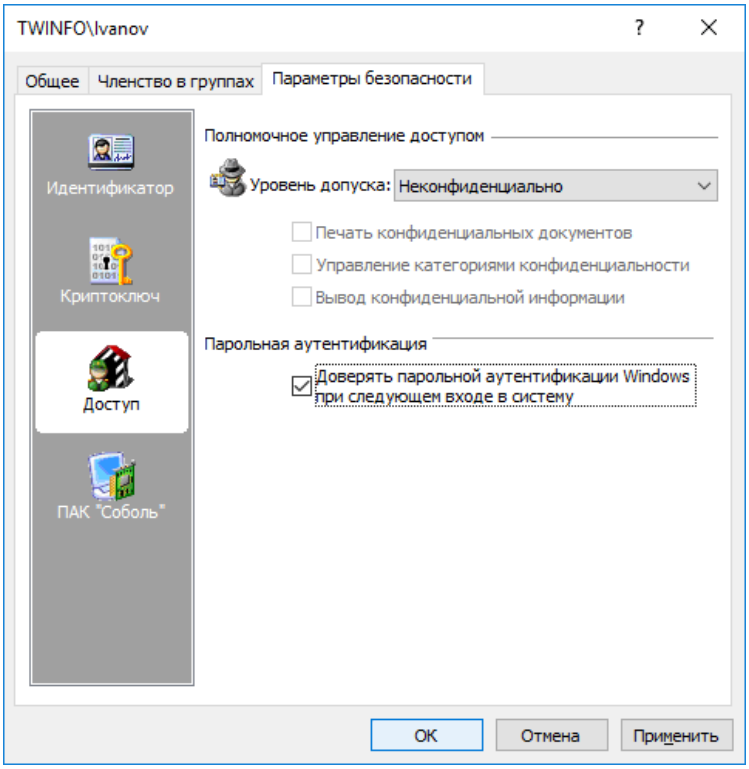
Назначение уровней допуска и привилегий пользователям

Уровень допуска и привилегии назначаются администратором безопасности каждому пользователю индивидуально.

Привилегию можно предоставить только тем пользователям, которым назначен уровень допуска.

Для назначения уровня допуска и привилегий:

1. Запустите программу управления пользователями (см. стр.270).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. В панели выбора групп параметров выберите группу "Доступ".



4. Установите уровень допуска пользователя в одноименном поле.

   Для уровня допуска, отличного от категории для общедоступной информации (по умолчанию — "Неконфиденциально"), становится доступным назначение привилегий.

5. Для предоставления или отмены привилегий пользователя установите или удалите отметки в соответствующих полях.

6. Нажмите кнопку "OK".

Примечание. Параметры вступят в силу при следующем входе пользователя в систему.

Присвоение категорий конфиденциальности ресурсам

Категорию конфиденциальности можно назначить для следующих ресурсов:

- устройства, для которых поддерживается разграничение доступа с использованием механизма полномочного управления доступом;
- каталоги и файлы на локальных физических дисках.

Присвоение категорий конфиденциальности устройствам

К устройствам, которым можно назначить категорию конфиденциальности, относятся локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, входящие в группы устройств USB, PCMCIA, IEEE1394 или SD.

Категории конфиденциальности можно присвоить:

- индивидуально каждому устройству;
- группе, классу или модели в списке устройств для наследования категории новыми устройствами (только категорию для общедоступной информации — "неконфиденциально").

Для присвоения категорий конфиденциальности объектам в списке устройств:

1. Загрузите список устройств (см. стр.85).
2. Выберите строку с нужным элементом списка (группа, класс, модель или устройство).

3. Укажите нужные параметры в ячейке колонки "Параметры доступа". Для этого нажмите кнопку в правой части ячейки. Если для класса или модели нужно явно задать параметры, удалите отметку из поля "Для новых устройств использовать настройки категории с родительского объекта". Для назначения категории конфиденциальности выберите нужную категорию (полный список категорий представлен только для конкретного устройства). Если устройство должно функционировать независимо от уровня допуска пользователя, отметьте поле "Без учета категории". Нажмите кнопку "Применить".
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Присвоение категорий конфиденциальности каталогам и файлам

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию "Управление категориями конфиденциальности".

Описание процедур изменения категорий конфиденциальности каталогов и файлов см. в документе [**3**].

Внимание! При присвоении ресурсам категорий конфиденциальности учитывайте следующие общие рекомендации:

- Не присваивайте категорию, отличную от категории для общедоступной информации (по умолчанию "неконфиденциально"), системным каталогам, каталогам, в которых размещается прикладное ПО, а также каталогу "Мои документы" и всем подобным ему.
- Во избежание непроизвольного повышения категорий конфиденциальности файлов храните файлы в каталогах с категорией конфиденциальности, равной категории конфиденциальности файлов. При этом учитывайте категорию конфиденциальности устройства, на котором располагаются эти объекты, так как категория устройства имеет более высокий приоритет.

Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма полномочного управления доступом, необходимо выполнить настройку регистрации событий. Настройка выполняется в Центре управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Полномочное управление доступом". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр.**162**) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

Настройка использования принтеров для печати документов

При необходимости можно ограничить использование принтеров для печати документов, которым присвоены определенные категории конфиденциальности. По умолчанию на всех принтерах разрешается печать документов с любой категорией конфиденциальности.

Категории конфиденциальности могут быть заданы для конкретных принтеров или для элемента "Настройки по умолчанию" в списке принтеров.

Также для принтеров предусмотрена возможность настройки прав пользователей для печати документов (см. стр.**101**).

Для настройки использования принтеров:

1. Загрузите список принтеров (см. стр.**98**).
2. Выберите строку с нужным элементом списка.
3. Укажите нужные параметры в ячейке колонки "Категории конфиденциальности". Для этого нажмите кнопку в правой части ячейки. Отметьте нужные уровни конфиденциальности.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка режима скрытия конфиденциальных файлов

Этот режим обеспечивает скрытие от пользователя в различных файловых менеджерах имен конфиденциальных файлов, доступ к которым ему запрещен.

После включения данного режима:

- при отключенном контроле потоков пользователь не будет видеть файлы, категория конфиденциальности которых выше его уровня допуска;
- при включенном контроле потоков пользователь, независимо от его уровня допуска, не увидит файлы, категория конфиденциальности которых выше уровня конфиденциальности текущей сессии.

При этом имена каталогов любой категории конфиденциальности отображаются всегда.

Ниже приведена процедура настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для включения или отключения режима:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полномочное управление доступом".
3. Для параметра "Режим скрытия" выберите вариант "Скрывать недоступные конфиденциальные файлы" либо вариант "Отображать недоступные конфиденциальные файлы".
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

В некоторых случаях может потребоваться вывести из-под действия механизма скрытия некоторые файлы и группы файлов. Это можно сделать, добавив такие ресурсы в список исключений в программе настройки подсистемы полномочного управления доступом (см. стр.**294**).

Дополнительная настройка для работы в режиме контроля потоков

Рекомендуемый порядок настройки

Для корректного функционирования системы при использовании механизма полномочного управления доступом в режиме контроля потоков рекомендуется выполнить настройку в следующем порядке:

1. Учетной записи администратора безопасности предоставьте возможность управления механизмом полномочного управления доступом. Для этого:
   - назначьте учетной записи наивысший уровень допуска к конфиденциальной информации и предоставьте привилегию "Управление категориями конфиденциальности" (см. стр.**163**);
   - включите администратора безопасности в локальные группы администраторов компьютеров.
2. На каждом компьютере выполните следующие действия:
   - создайте профили всех пользователей, которые будут работать на компьютере. Профиль пользователя автоматически формируется операционной системой при первом входе в систему (если ранее пользователь не выполнял вход на данном компьютере);
   - выполните запуск приложений, которые будут использоваться, и настройте параметры работы приложений;

- запустите программу настройки для режима контроля потоков (см. стр.**167**), включите режим автоматической настройки для нужных приложений и выполните автоматическую настройку.

3. Укажите уровни конфиденциальности для сетевых интерфейсов (см. стр.**168**).
4. Включите режим контроля потоков (см. стр.**168**).
5. Проверьте на компьютерах корректность функционирования приложений в конфиденциальных сессиях. При возникновении ошибок выполните действия для настройки совместного функционирования с прикладным ПО (см. стр.**169**).

Программа настройки для режима контроля потоков

Чтобы обеспечить функционирование механизма полномочного управления доступом при включенном режиме контроля потоков, требуется выполнить дополнительную настройку локально на компьютере. Для этого используется программа настройки подсистемы полномочного управления доступом для режима контроля потоков (далее — программа настройки для режима контроля потоков, программа настройки). Настройка выполняется перед включением режима контроля потоков, а также в процессе эксплуатации системы при добавлении новых пользователей, программ, принтеров, для оптимизации функционирования механизма.

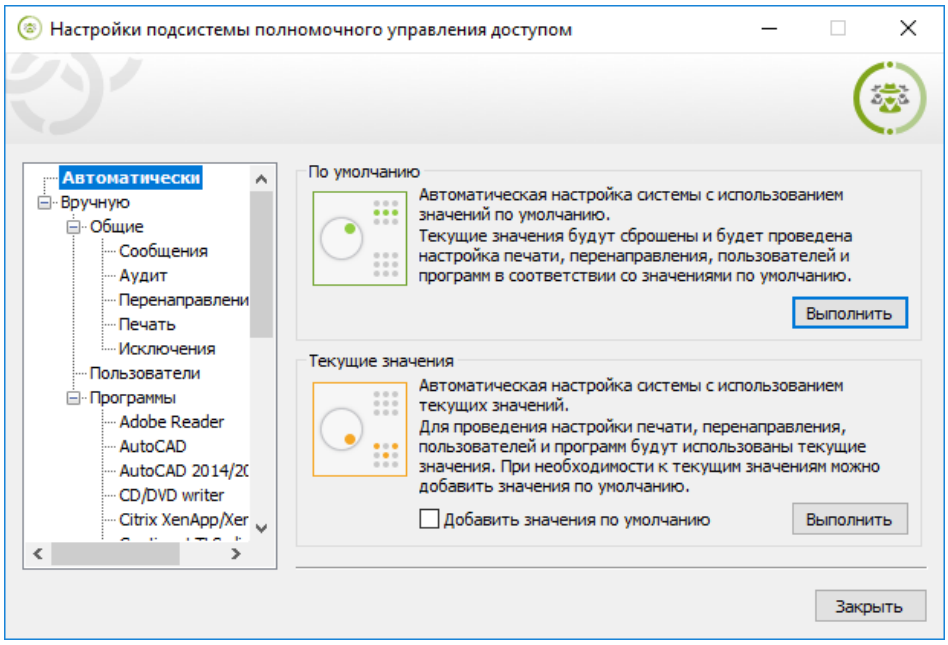
Для запуска программы:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Программа настройки подсистемы полномочного управления доступом".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора.
2. В поле "PIN администратора" введите PIN администратора и нажмите кнопку "ОК".

Примечание. Программа будет запущена в режиме просмотра настроек в следующих случаях:
- если текущий пользователь не входит в локальную группу администраторов;
- если механизм полномочного управления доступом отключен.

Пример содержимого окна программы представлен на рисунке ниже.



Программа может функционировать в обычном режиме, который предоставляет все возможности для редактирования и настройки, или в режиме просмотра текущего состояния параметров (только чтение). Запуск программы в обычном режиме осуществляется при следующих условиях:

- пользователю назначен наивысший уровень допуска к конфиденциальной информации;
- пользователю предоставлена привилегия "Управление категориями конфиденциальности";
- режим контроля потоков отключен.

При невыполнении хотя бы одного из перечисленных условий запуск программы возможен только в режиме просмотра текущего состояния параметров.

В программе реализованы средства как для автоматической настройки, так и для конфигурирования вручную. При автоматической настройке выполняется базовый набор действий, после которых обеспечивается функционирование механизма и совместимость со стандартным и наиболее распространенным программным обеспечением. Средства запуска автоматической настройки представлены в окне программы по умолчанию. Настройка вручную предусмотрена для выполнения специфических действий — например, чтобы обеспечить совместную работу с ПО, которое не входит в список для автоматической настройки.

Подробные сведения о работе с программой приведены в приложении на стр.**287**.

Выбор уровней конфиденциальности для сетевых интерфейсов

При настройке параметров сетевого интерфейса можно указать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователям в режиме контроля потоков.

Для настройки использования интерфейсов при контроле потоков:

1. Загрузите список устройств (см. стр.**85**).
2. В группе "Сеть" выберите строку с нужным элементом списка (группа, класс или сетевой интерфейс).
3. Укажите нужные параметры в ячейке колонки "Параметры доступа". Для этого нажмите кнопку в правой части ячейки. Если для класса или модели нужно явно задать параметры, удалите отметку из поля "Для новых устройств использовать настройки категории с родительского объекта". Отметьте нужные уровни конфиденциальности. Чтобы устройство функционировало независимо от уровня конфиденциальности сессии, удалите отметки для всех уровней. Нажмите кнопку "Применить".
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Включение и отключение режима контроля потоков

Ниже приводятся описания процедур централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для включения режима контроля потоков:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полномочное управление доступом".
3. Для параметра "Режим работы" установите отметку в поле "Контроль потоков включен" и при необходимости настройте параметры автоматического назначения уровней конфиденциальности для сессий пользователей:

- чтобы ограничить выбор уровней конфиденциальности для терминальных подключений — установите отметку в поле "Строгий контроль терминальных подключений". В этом случае уровень конфиденциальности терминальной сессии будет устанавливаться равным уровню конфиденциальности локальной сессии на терминальном клиенте (соответственно, режим контроля потоков также должен быть включен на клиенте);
- чтобы включить принудительное назначение максимально возможных уровней конфиденциальности для сессий пользователей — установите отметку в поле "Автоматический выбор максимального уровня сессии". В этом случае сессии будет назначаться уровень конфиденциальности, равный уровню допуска пользователя, который выполняет вход в систему.

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Для отключения режима контроля потоков:

1. Выполните вход в систему в неконфиденциальной сессии.
2. Выполните действия **1**, **2** вышеописанной процедуры.
3. Для параметра "Режим работы" установите отметку в поле "Контроль потоков отключен".
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Порядок настройки совместного функционирования с прикладным ПО

При работе механизма полномочного управления доступом в режиме контроля потоков могут происходить сбои запуска или функционирования некоторых приложений прикладного программного обеспечения. Если сбои проявляются только при работе с приложением в конфиденциальных сессиях (с уровнем выше чем "неконфиденциально"), это может происходить по причине запрета обращения к файлам приложения со стороны механизма.

Чтобы обеспечить корректную работу приложений, для режима контроля потоков предусмотрена функция перенаправления вывода служебных файлов. Для применения функции создаются копии отдельных служебных каталогов приложений с различными категориями конфиденциальности. В зависимости от уровня конфиденциальности сессии файловые операции прикладного ПО автоматически перенаправляются в каталог-копию с соответствующей категорией конфиденциальности. Таким образом, для приложения реализуется возможность работы со служебными каталогами и при этом данные сохраняются с нужной категорией конфиденциальности.

Если после включения режима контроля потоков приложение перестает корректно функционировать, выполните следующие действия для диагностики и настройки совместного функционирования:

1. Проверьте наличие готового шаблона настройки для работы данного приложения. Для этого запустите программу настройки (см. стр.**167**) и перейдите к разделу "Вручную | Программы". Если приложение присутствует в списке, включите для него режим автоматической настройки и затем выполните автоматическую настройку с текущими значениями параметров. При отсутствии приложения перейдите к следующим действиям для диагностики и настройки.

   Примечание. Список приложений в программе настройки предназначен для применения готовых шаблонов настройки совместной работы. По умолчанию режим автоматической настройки отключен для большинства элементов списка (например, для ПО AutoCAD, Photoshop и др.). Поэтому для применения шаблона данный режим необходимо включить. Подробные сведения о работе с программой приведены в приложении на стр.**287**.

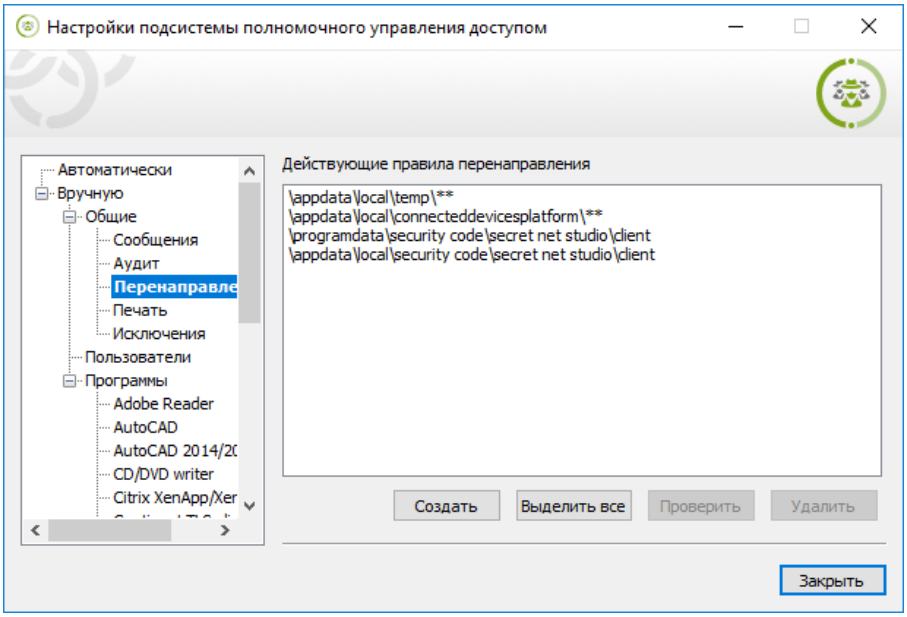
2. Выполните вход в систему с отключенным режимом контроля потоков или в неконфиденциальной сессии. Запустите Локальный центр управления и выполните очистку локального журнала Secret Net Studio.

3. Завершите сеанс, включите режим контроля потоков и выполните вход в конфиденциальной сессии.
4. Запустите приложение. Если запуск выполняется успешно, воспроизведите действия, которые приводят к ошибкам в работе ПО.
5. Завершите сеанс, выполните вход в неконфиденциальной сессии и отключите режим контроля потоков.
6. Запустите Локальный центр управления и загрузите записи журнала Secret Net Studio. Найдите записи о событиях запрета доступа категории "Полномочное управление доступом". В дополнительных описаниях событий определите процессы, относящиеся к приложению, и пути, по которым выполнялись обращения.
7. Проанализируйте полученные пути и по возможности классифицируйте их, исходя из назначения каталогов. Каталоги, в которых могут происходить сбои при обращении к файлам:

Каталоги с документами пользователей
В каталогах хранятся файлы рабочих документов пользователей. Например, каталог \Documents в профиле пользователя. Вероятные причины запрета доступа — не соблюдаются общие рекомендации по присвоению категорий каталогам и файлам (см. стр.**165**) или действуют правила работы с конфиденциальными ресурсами (см. стр.**172**). Применять перенаправление для таких каталогов не рекомендуется. Для обеспечения доступа следует установить корректные категории конфиденциальности ресурсов (обеспечить соответствие категорий каталогов и хранящихся в них файлов)

Каталоги временных данных приложения
Каталоги используются приложением для записи и чтения временных данных в течение одного сеанса работы. После завершения сеанса созданные файлы, как правило, удаляются. Вероятная причина запрета доступа — произошла попытка создания файла в каталоге, для которого установлена категория конфиденциальности ниже, чем уровень сессии. В большинстве случаев перенаправление для таких каталогов не требуется. Достаточно установить максимальную категорию конфиденциальности без автоматического присвоения категории для создаваемых объектов. За счет этого приложению будет разрешено создание файлов в сессиях любых уровней конфиденциальности
Каталоги с параметрами настройки приложения
В каталогах хранятся конфигурационные файлы, которые формируются приложением при первом запуске и настройке и в дальнейшем не изменяются при обычной работе приложения. Доступ к таким файлам во всех следующих сеансах осуществляется только на чтение для загрузки параметров приложения. Вероятная причина запрета доступа — произошла попытка создания или модификации конфигурационных файлов в каталоге, который был создан при настройке параметров приложения. В большинстве случаев перенаправление для таких каталогов не требуется. При необходимости изменить конфигурационные файлы выполните настройку приложения в неконфиденциальной сессии
Каталоги с рабочими данными приложения
Каталоги используются приложением для записи и чтения служебных данных в каждом сеансе работы. Файлы не удаляются после завершения сеанса и могут перезаписываться в следующих сеансах. Корректная работа с файлами в таких каталогах обеспечивается с помощью функции перенаправления (см. ниже)

8. Для создания правил перенаправления запустите программу настройки и перейдите к разделу "Вручную | Общие | Перенаправление".



Добавление правил осуществляется с помощью кнопки "Создать". Каждое правило перенаправления должно содержать часть пути, которая идентифицирует перенаправляемые каталоги. Например, значение \AppData\Local\Temp** соответствует временному каталогу в профиле пользователя. Каталоги, у которых часть пути совпадает с указанным значением, будут перенаправляться в конфиденциальных сессиях. В приведенном примере правило обеспечивает перенаправление временных каталогов (со всеми подкаталогами) всех пользователей компьютера.

Рекомендации для формирования списка правил перенаправления

- По возможности избегайте копирования больших объемов данных из исходных каталогов в каталоги перенаправления. При настройке функции перенаправления из исходных каталогов вместо дублирования всего содержимого можно копировать только подкаталоги без файлов или только вложенные файлы без каталогов. Такое копирование осуществляется, если в правиле перенаправления в конце пути указана шаблонная подстрока "**" (с двумя символами "звездочка") или "*" (с одним символом "звездочка") соответственно.
- Часть пути в правиле перенаправления следует задать с оптимальной точностью для идентификации каталогов. Обычно достаточно указать каталоги двух-трех уровней вложенности. Слишком короткая часть пути может привести к перенаправлению каталогов, не относящихся к нужному приложению. Излишне подробное значение может вызвать необходимость создания отдельных правил (например, для каждого пользователя). Это усложнит настройку, а также повлияет на скорость обработки данных подсистемой.

9. Включите режим контроля потоков, выполните вход в конфиденциальной сессии и убедитесь в корректном функционировании приложения. Если данное приложение будет использоваться на других компьютерах с включенным режимом контроля потоков, выполните локальную настройку использования тех же каталогов (см. действия **7**, **8**).

Правила работы с конфиденциальными ресурсами

Данный раздел содержит обобщенные правила работы с конфиденциальными ресурсами в условиях работающего механизма полномочного управления доступом. В таблице приведены правила работы, действующие при отключенном и включенном режимах контроля потоков конфиденциальной информации.

Без контроля потоков	При контроле потоков
Доступ к устройствам	
Запрещен вход пользователя в систему, если подключены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя	Запрещен вход пользователя в систему, если подключены устройства: • с категорией конфиденциальности выше, чем уровень допуска пользователя; • с различными категориями конфиденциальности; • с категорией конфиденциальности выше, чем категория "неконфиденциально", при первом входе пользователя на данном компьютере (конфигурационный вход)
Запрещено подключение устройства, если его категория конфиденциальности выше, чем уровень допуска работающего пользователя	Запрещено подключение устройства, если его категория конфиденциальности отличается от уровня сессии работающего пользователя
Разрешено функционирование всех сетевых интерфейсов	Запрещено использование сетевых интерфейсов, для которых текущий уровень конфиденциальности сессии не указан в списке разрешенных уровней
Отсутствуют ограничения по доступу к устройствам, для которых включен режим доступа "без учета категории конфиденциальности"	
Доступ к файлам	
Если задана категория конфиденциальности для устройства, содержащего файл, при доступе к этому файлу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности файла	
Запрещен доступ к файлу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего файл	

Без контроля потоков	При контроле потоков
Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла	Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла
Запрещено удаление конфиденциального файла с помещением в "Корзину"	Запрещено удаление любого файла с помещением в "Корзину"
Доступ к каталогам	
Если задана категория конфиденциальности для устройства, содержащего каталог, при доступе к этому каталогу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности каталога	
Запрещен доступ к каталогу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего каталог	
Конфиденциальные файлы размещаются в каталогах, имеющих категорию конфиденциальности не ниже категории конфиденциальности файла. Например, в каталоге с категорией "конфиденциально" могут размещаться как неконфиденциальные файлы, так и файлы с категорией "конфиденциально"	
Пользователь, не имеющий доступ к файлу, может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть файл. Поэтому названия конфиденциальных файлов не должны содержать конфиденциальную информацию	
Запрещено удаление конфиденциального каталога с помещением в "Корзину"	Запрещено удаление любого каталога с помещением в "Корзину"
Наследование категории конфиденциальности каталога	
Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении (перезаписи), копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога	Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении, копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога. Ограничение: устанавливаемая категория конфиденциальности должна быть равна текущему уровню конфиденциальности сессии
Если отключен режим автоматического присвоения категории конфиденциальности: • при создании, сохранении или копировании подкаталогу/файлу присваивается категория "неконфиденциально"; • при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности вышестоящего каталога). Для перемещения подкаталогов требуется соответствующая привилегия пользователя	Если отключен режим автоматического присвоения категории конфиденциальности: • при создании, сохранении или копировании подкаталогу/файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога; • при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение подкаталога/файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога и уровень конфиденциальности сессии)

Без контроля потоков	При контроле потоков
Каталоги с отключенным режимом автоматического присвоения категории конфиденциальности целесообразно использовать для хранения файлов с различными категориями конфиденциальности (меньшими или равными категории конфиденциальности каталога). Чтобы исключить неожиданное изменение категорий конфиденциальности файлов после выполнения операций с ними, рекомендуется использовать каталоги, для которых установлено одинаковое состояние режима автоматического присвоения категории конфиденциальности	
Работа в приложениях	
Приложению присваивается уровень конфиденциальности, равный наивысшей категории конфиденциальности среди открытых в приложении файлов. Уровень конфиденциальности приложения не снижается после закрытия конфиденциального файла и сохраняется до закрытия приложения	Приложению присваивается уровень конфиденциальности, равный текущему уровню сессии пользователя. Разрешается открывать файлы не выше этого уровня. Категория файлов с более низким уровнем конфиденциальности повышается до уровня конфиденциальности сессии (повышение категории происходит при сохранении файла)
Некоторые приложения при запуске автоматически обращаются к определенным файлам. Например, к ранее открывавшимся файлам в приложении. При этом не происходит непосредственное открытие файла (документа). В силу особенностей механизма полномочного управления доступом при таких обращениях к конфиденциальным файлам пользователю предлагается повысить уровень конфиденциальности приложения до категории файлов. В таких случаях, если не планируется работать с предложенным уровнем конфиденциальности, достаточно отказаться от повышения уровня конфиденциальности приложения	
Изменение категории конфиденциальности ресурса	
Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше своего уровня допуска (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)	Пользователь, **не** обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше уровня конфиденциальности сессии (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)
Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше уровня допуска пользователя; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше уровня допуска пользователя; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше уровня допуска пользователя	Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: • повысить категорию конфиденциальности каталогов и файлов, но не выше текущего уровня сессии; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше текущего уровня сессии; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше текущего уровня сессии

<table>
<tr><th colspan="2">Печать конфиденциальных документов</th></tr>
<tr><td>Если включен механизм контроля печати:
пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы;
пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей уровень допуска пользователя</td><td>Если включен механизм контроля печати:
пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (при условии, что документ не редактировался);
пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей текущий уровень сессии</td></tr>
<tr><td colspan="2">Если отключен механизм контроля печати, любому пользователю, имеющему доступ к конфиденциальным документам, разрешен вывод этих документов на печать независимо от наличия у него привилегии "Печать конфиденциальных документов". При этом документы распечатываются без грифа конфиденциальности</td></tr>
<tr><th colspan="2">Вывод на внешние носители</th></tr>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><td>Пользователь, имеющий доступ к конфиденциальным документам, может копировать файлы или сохранять их содержимое на любые носители независимо от наличия привилегии "Вывод конфиденциальной информации"</td><td>Пользователь, не обладающий привилегией "Вывод конфиденциальной информации", не может копировать конфиденциальные файлы или сохранять их содержимое на внешние носители</td></tr>
</table>

Глава 12
Дискреционное управление доступом к каталогам и файлам

При настройке дискреционного разграничения доступа пользователей к каталогам и файлам на локальных дисках выполняются действия:

1. Предоставление привилегии для изменения прав доступа на любых ресурсах (см. ниже).
2. Назначение администраторов ресурсов (см. стр.**176**).
3. Настройка регистрации событий и аудита операций с ресурсами (см. стр.**177**).

Предоставление привилегии для изменения прав доступа к ресурсам

В механизме дискреционного управления доступом предусмотрена возможность для привилегированных пользователей изменять права доступа на любых каталогах и файлах локальных дисков независимо от установленных прав доступа к самим ресурсам. Для этого пользователю должна быть предоставлена привилегия "Управление правами доступа". Привилегия, в частности, позволяет назначить администраторов ресурсов, которые в дальнейшем смогут настраивать права доступа к ресурсам для остальных пользователей.

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в локальную группу администраторов.

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для предоставления привилегии:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Дискреционное управление доступом".
3. Для параметра "Учетные записи с привилегией управления правами доступа" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Назначение администраторов ресурсов

Администраторы ресурсов в механизме дискреционного управления доступом могут изменять права доступа других пользователей к определенным каталогам и файлам на локальных дисках. Администратором ресурса считается пользователь, для которого установлено разрешение на операцию "Изменение прав доступа" в параметрах доступа к ресурсу. Описание процедуры изменения прав доступа см. в разделе "Изменение прав доступа к каталогам и файлам" документа [**3**].

Настройка регистрации событий и аудита операций с ресурсами

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма дискреционного управления доступом к каталогам и файлам, необходимо выполнить настройку регистрации событий. Настройка выполняется в Центре управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Дискреционное управление доступом". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр. **176**) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

Настройка аудита успехов и отказов

Настройка параметров аудита операций с ресурсом выполняется при изменении прав доступа к этому ресурсу. Описание процедуры изменения прав доступа см. в разделе "Изменение прав доступа к каталогам и файлам" документа [**3**].

Глава 13
Защита локальных дисков

Защита доступа к локальным дискам (логическим разделам) компьютера осуществляется с использованием механизма защиты дисков Secret Net Studio. Механизм блокирует доступ к дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным клиентским ПО Secret Net Studio. Все другие способы загрузки ОС считаются несанкционированными с точки зрения функционирования механизма (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).

Процедура настройки механизма защиты дисков состоит из следующих этапов:

1. Включение механизма (см. ниже).
2. Включение/отключение защиты логических разделов (см. стр.**180**).

Инструкция по отключению механизма защиты дисков приведена на стр.**181**.

Имеется возможность восстановления данных на дисках, защищенных с помощью механизма защиты дисков Secret Net Studio, с помощью диска аварийного восстановления (см. стр.**299**).

Включение механизма защиты дисков

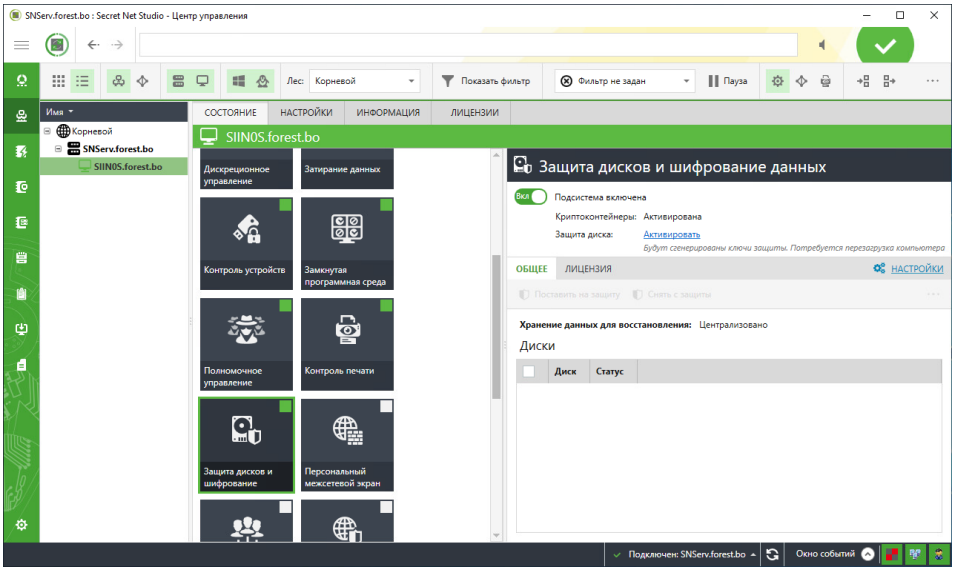
По умолчанию после установки клиентского ПО Secret Net Studio и регистрации лицензии механизм защиты дисков отключен. Процедура включения выполняется администратором.

При включении механизма генерируется файл восстановления, содержащий специальный ключ, на основе которого в дальнейшем будут модифицироваться загрузочные секторы (boot-секторы) логических разделов на жестких дисках компьютера. Генерация нового файла выполняется в обязательном порядке при включении механизма на данном компьютере. Если включен централизованный режим хранения данных восстановления, то файл хранится на сервере безопасности. Если централизованный режим хранения отключен, то файл восстановления может быть создан на локальном компьютере, сменном носителе или сетевом ресурсе, а затем его можно свободно копировать. Если централизованный режим хранения отключен, то файл восстановления создается на локальном компьютере.

Внимание! Если системный диск (физический диск, с которого выполняется загрузка ОС) использует основную загрузочную запись (MBR), в настройках BIOS компьютера должна быть отключена функция проверки загрузочных вирусов. Для отключения функции установите значение "Disabled" для параметра "Boot Virus Detection" (наличие данной функции и название параметра зависит от используемой версии BIOS).

Для централизованного включения механизма защиты дисков:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Хранение данных восстановления/Хранение данных восстановления для системных и несистемных разделов". Установите отметку в поле "Хранить централизованно".
3. Перейдите на вкладку "Состояние" и выберите плитку "Защита дисков и шифрование". Справа отобразится блок с информацией о механизме.

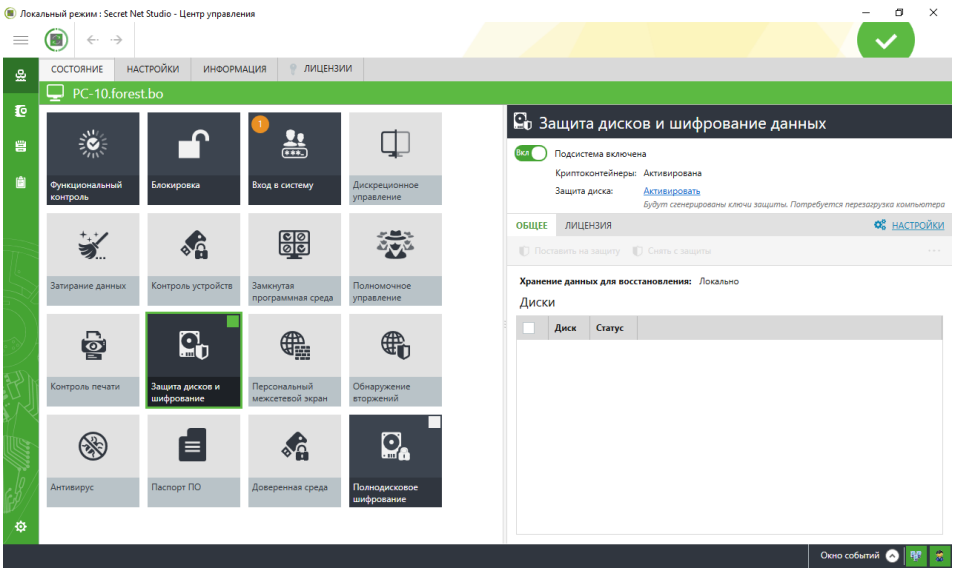


В поле "Защита диска" нажмите ссылку "Активировать".

4. После включения механизма перезагрузите компьютер и дождитесь завершения процесса загрузки ОС.

Для локального включения механизма защиты дисков:

1. В Локальном центре управления перейдите на вкладку "Состояние" и выберите плитку "Защита дисков и шифрование". Справа отобразится блок с информацией о механизме.



В поле "Защита диска" нажмите ссылку "Активировать".

2. После включения механизма перезагрузите компьютер и дождитесь завершения процесса загрузки ОС.

   При первом включении механизма защиты дисков после загрузки ОС появится диалоговое окно с запросом пути для сохранения файла восстановления.

3. Выберите путь для сохранения файла восстановления и нажмите кнопку "Готово".

Примечание. Если на компьютере установлен ПАК "Соболь", в котором включен контроль целостности физических секторов жесткого диска, после включения механизма защиты дисков ПАК "Соболь" может зафиксировать нарушение целостности загрузочного сектора. В этом случае для устранения ошибок КЦ необходимо средствами ПАК "Соболь" выполнить новый расчет эталонных контрольных сумм.

Включение и отключение защиты логических разделов

По умолчанию после включения механизма защиты дисков режим защиты отключен для всех логических разделов. Включение режима защиты нужных разделов осуществляется выборочно.

Механизм обеспечивает защиту до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему FAT, NTFS или ReFS. Поддерживаются физические диски с MBR или с таблицей разделов на идентификаторах GUID Partition Table (GPT). Диски с другими типами разбиения на логические разделы не поддерживаются (например, динамические диски).

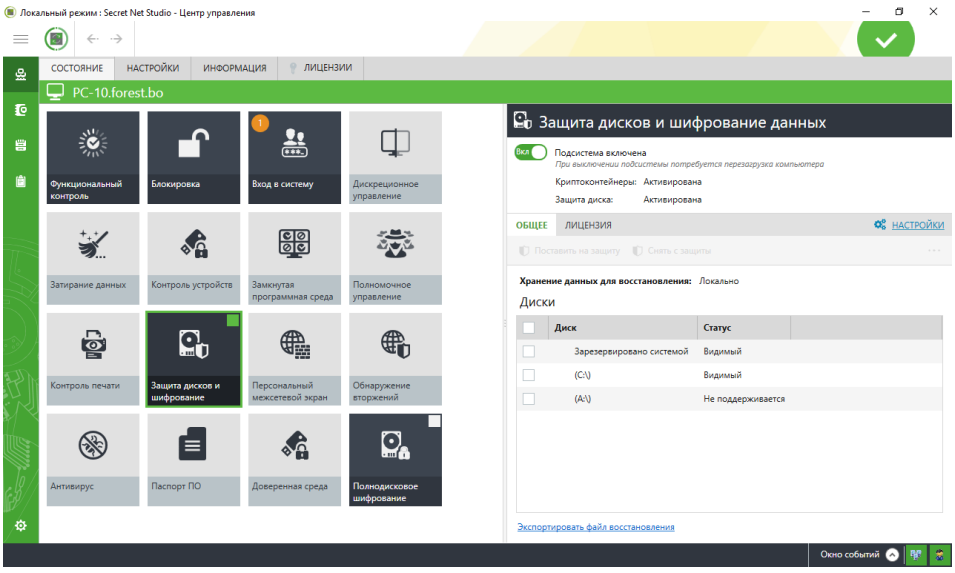
Ниже приводится описание процедур включения и отключения защиты логических разделов при работе с Центром управления. Включение и отключение защиты дисков локально выполняется аналогично с использованием Локального центра управления.

Примечание. Для централизованного включения и отключения защиты дисков требуется, чтобы был включен централизованный режим хранения данных восстановления (см. стр.178)

Для включения/отключения режима защиты:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Состояние" и выберите плитку "Защита дисков и шифрование".

   Справа отобразится список дисков, для которых можно включить режим защиты.



2. Отметьте логические разделы, для которых необходимо включить режим защиты и нажмите кнопку "Поставить на защиту". Если необходимо отключить защиту логического раздела, удалите отметку слева от его названия и нажмите кнопку "Снять с защиты".

Отключение механизма защиты дисков

Перед отключением механизма защиты дисков необходимо снять защиту со всех логических разделов. При этом ключ не удаляется из системы и может использоваться повторно на данном компьютере. Ниже приводится описание процедуры отключения механизма защиты дисков при работе с Центром управления. Включение и отключение механизма защиты дисков локально выполняется аналогично с использованием Локального центра управления.

Для отключения механизма защиты дисков:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Состояние" и выберите плитку "Защита дисков и шифрование". Справа отобразится блок с информацией о механизме.
2. Переведите в положение "Выкл" выключатель, расположенный слева в заголовке блока. Произойдет отключение механизма, после чего появится сообщение "Требуется перезагрузка компьютера".
3. После отключения механизма перезагрузите компьютер.

Глава 14
Шифрование данных на дисках

Механизм полнодискового шифрования Secret Net Studio позволяет шифровать данные на носителях информации для предотвращения попыток несанкционированного доступа к конфиденциальной информации, хранящейся на этих носителях.

Поддерживается шифрование системных и несистемных разделов жестких дисков со структурой разделов GPT и режимом загрузки UEFI, а также шифрование несистемных разделов жестких дисков со структурой разделов MBR.

Максимальное количество зашифрованных разделов на одном жестком диске — 32. Количество жестких дисков не ограничено. Максимальное полное количество зашифрованных разделов на всех жестких дисках — 66.

Пояснение. В указанные ограничения также входят разделы, защищенные с помощью механизма защиты диска Secret Net Studio.

Шифрование выполняется по алгоритму AES-256. Ключевая информация хранится в зашифрованном виде на незашифрованном разделе ESP (EFI System Partition) и включает в себя:

- ключ шифрования — ключ, с помощью которого шифруются данные на дисках;
- ключ домена безопасности — ключ, с помощью которого шифруются данные для восстановления доступа к зашифрованным дискам (далее – данные восстановления).

Для получения доступа к зашифрованным дискам необходим пароль, установленный при шифровании данных. Шифрование нескольких дисков осуществляется с одним паролем доступа.

Операции механизма полнодискового шифрования могут быть запущены:

- локально на компьютере с использованием программы "Шифрование и защита диска Secret Net Studio" (далее – мастер шифрования);
- локально на компьютере с использованием Локального центра управления;
- централизованно для одного или нескольких компьютеров с использованием Центра управления.

Шифрование данных доступно пользователям и группам пользователей, которым предоставлена привилегия на шифрование.

При включении подсистемы полнодискового шифрования на компьютер устанавливается загрузчик Secret Net Studio. Если на компьютере имеются зашифрованные диски, при включении компьютера стартует загрузчик Secret Net Studio и запрашивается пароль доступа к дискам. Также становятся доступными операции восстановления доступа к дискам.

Пояснение.

- Более подробное описание возможностей и ограничений подсистемы полнодискового шифрования приведено в документе "Руководство администратора. Установка, управление, мониторинг и аудит" (раздел "Шифрование данных на дисках").
- Инструкции по работе на компьютере с зашифрованными дисками приведены в документе [3] (раздел "Шифрование данных на дисках").

Настройка параметров шифрования

Шифрование данных доступно пользователям и группам пользователей, которым предоставлена привилегия на шифрование.

Привилегия на шифрование предоставляется в Центре управления (централизованная настройка) или в Локальном центре управления (локальная настройка) администратором, имеющим привилегию на редактирование политик.

Параметры подсистемы полнодискового шифрования настраиваются в Центре управления (централизованная настройка) или в Локальном центре управления (локальная настройка). Администратор, выполняющий настройку, должен иметь привилегию на редактирование политик.

Ниже приводится описание процедур предоставления привилегии на локальное шифрование и настройку параметров, выполняющихся централизованно. Локально процедуры выполняются аналогично.

Для предоставления привилегии на шифрование:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полнодисковое шифрование".
3. Отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия шифрования данных на дисках, с помощью параметра "Учетные записи с привилегией на шифрование логических разделов жестких дисков".

   По умолчанию привилегией обладают пользователи, входящие в группу локальных администраторов.

Для настройки параметров шифрования:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полнодисковое шифрование".
3. Настройте режим шифрования системных и несистемных разделов дисков компьютера, установив для параметров "Шифрование системных разделов" и "Шифрование несистемных разделов" одно из следующих значений:
   - "Определяется пользователем" (значение по умолчанию)— пользователь имеет возможность зашифровывать и расшифровывать разделы самостоятельно, используя мастер шифрования.
   - "Шифровать" — разделы будут принудительно зашифрованы с предварительным уведомлением на компьютере. Локальное расшифрование запрещено.
   - "Не шифровать" — разделы, зашифрованные ранее, будут принудительно расшифрованы с предварительным уведомлением на компьютере. Локальное шифрование запрещено.
4. При необходимости настройте режим хранения данных восстановления на сервере безопасности. Для этого в разделе "Политики" перейдите к группе параметров "Хранение данных восстановления" и для параметра "Хранение данных восстановления для системных и несистемных разделов" установите отметку "Хранить централизованно".

   Примечания.
   - Политика доступна только для клиентов в сетевом режиме функционирования.
   - При переводе компьютера в автономный режим работы данные для восстановления будут храниться локально.
   - Политика распространяется также на механизм защиты дисков.
5. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Включение подсистемы полнодискового шифрования

По умолчанию после установки клиентского ПО Secret Net Studio и регистрации лицензии подсистема полнодискового шифрования отключена. Процедура включения выполняется администратором, обладающим привилегией на включение/отключение подсистем Secret Net Studio.

Пояснение. Отключить подсистему можно только при отсутствии зашифрованных дисков.

Ниже приводится описание процедуры централизованного включения подсистемы в Центре управления. Локальное включение выполняется аналогично в Локальном центре управления.

Для включения подсистемы:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо включить подсистему. На вкладке "Состояние" выберите элемент "Полнодисковое шифрование".
2. Переключите тумблер "Подсистема выключена" в положение "Вкл".

   Появится предупреждение о необходимости перезагрузки компьютера.
3. Перезагрузите компьютер.

   При перезагрузке будет установлен загрузчик Secret Net Studio. При успешной установке загрузчика Secret Net Studio подсистема будет включена.

   Ошибки при включении подсистемы могут возникнуть из-за несоответствия компьютера требованиям. Системные требования для функционирования подсистемы полнодискового шифрования приведены на стр.**182**.

Примечание. Включить подсистему централизованно можно также в табличном отображении структуры ОУ. Вызовите контекстное меню нужного компьютера, в пункте "Включение подсистем" выберите подсистему "Полнодисковое шифрование" и выберите команду "Включить".

Шифрование и расшифрование данных

В данном разделе описаны следующие процедуры:

- локальное шифрование данных администратором в мастере шифрования при локальном хранении данных восстановления (см. стр.**184**);
- локальное шифрование данных администратором в мастере шифрования при централизованном хранении данных восстановления (см. стр.**187**);
- локальное расшифрование данных в мастере шифрования (см. стр.**188**);
- шифрование и расшифрование данных в Центре управления (см. стр.**189**).

Локальное шифрование при локальном хранении данных восстановления

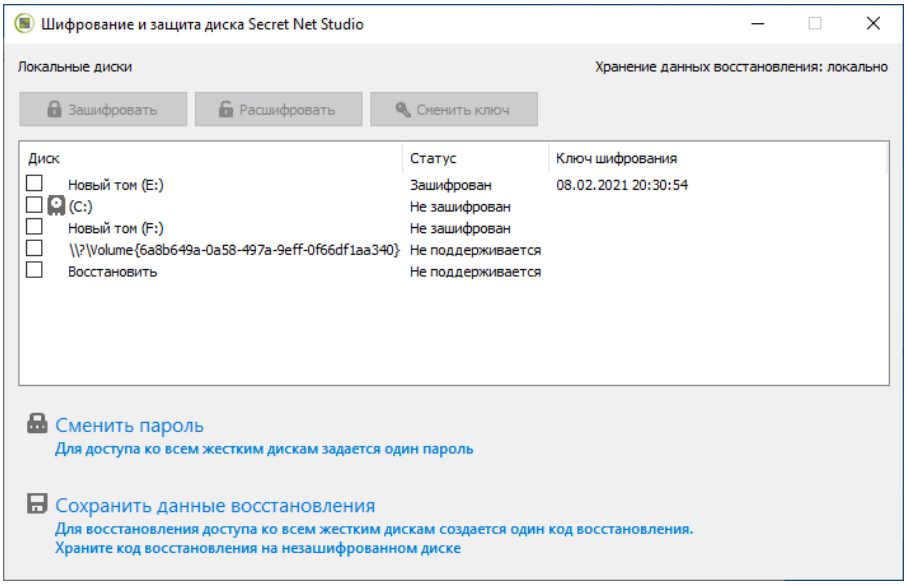
Локальное шифрование выполняется с использованием мастера шифрования Secret Net Studio на компьютере, диски которого необходимо зашифровать. Пользователь, выполняющий шифрование, должен иметь привилегию на шифрование (см. стр.**182**).

При необходимости можно сохранить файл восстановления, необходимый для создания диска аварийного восстановления. Диск позволяет восстановить доступ к зашифрованным разделам диска. В файле содержится вся необходимая информация для полного восстановления доступа при утрате пароля доступа или повреждении носителя.

Для шифрования:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Выберите команду "Шифрование".

   Появится окно мастера шифрования Secret Net Studio, подобное представленному на рисунке ниже.



Пояснение. Операцию шифрования можно запустить из контекстного меню диска. В пункте "Шифрование" выберите команду "Зашифровать" и перейдите к п. **4** данной инструкции.

2. Выберите диск, который необходимо зашифровать.

Пояснение.

- Имеется возможность шифрования нескольких дисков одновременно. Все диски компьютера шифруются с одним паролем доступа.
- Системный диск обозначается пиктограммой .
- Диск со статусом "Не поддерживается" зашифровать нельзя. Требования к дискам, поддерживаемых подсистемой полнодискового шифрования, приведены на стр.182.

3. Нажмите кнопку "Зашифровать".

Появится окно с запросом пароля доступа.

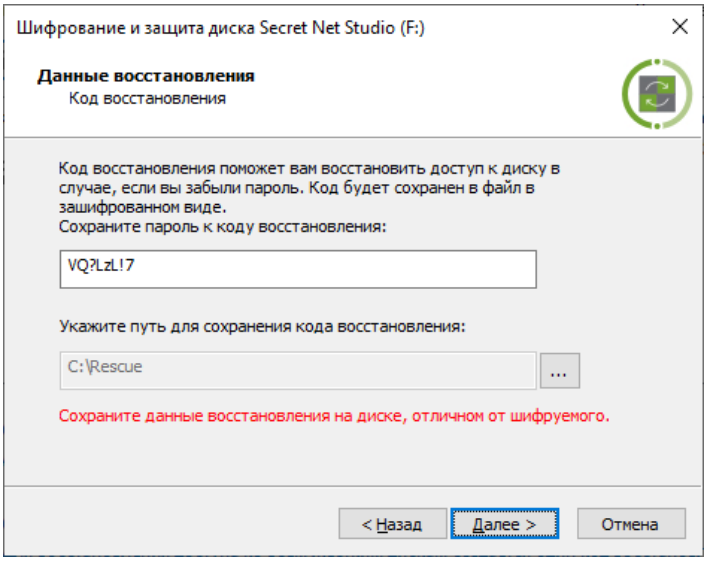
4. Установите пароль доступа к диску или введите пароль к ранее зашифрованным дискам компьютера.

Пояснение. Пароль доступа должен удовлетворять требованиям, указанным в окне запроса пароля.

При необходимости установите отметку в поле "сменить пароль при первом доступе к зашифрованным дискам". В этом случае пользователь должен будет сменить пароль доступа при первой загрузке системы с зашифрованным диском.

5. Нажмите кнопку "Далее".

Появится окно сохранения кода восстановления, подобное представленному на рисунке ниже.



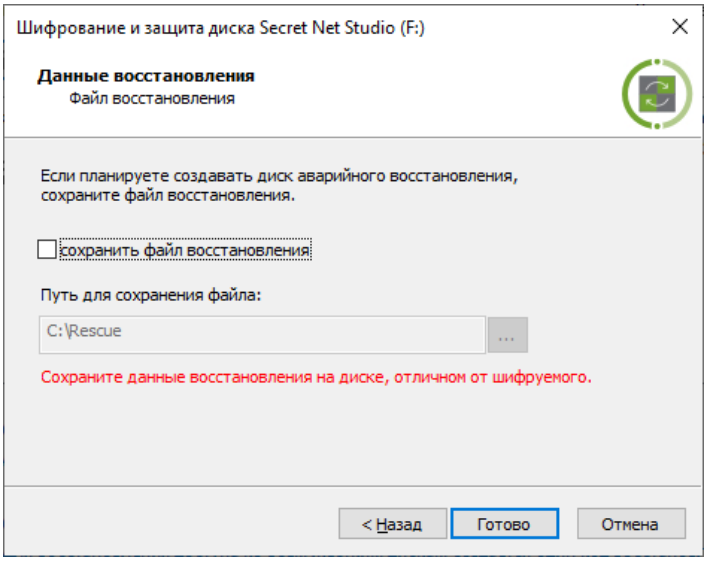
6. Сохраните пароль к коду восстановления, сгенерированный системой. Укажите путь для сохранения кода восстановления.

Внимание! Сохраните данные восстановления на диске, отличном от шифруемого.

Пояснение. Код восстановления можно сохранить повторно позже (см. стр.195).

7. Нажмите кнопку "Далее".

Появится окно сохранения файла восстановления, подобное представленному на рисунке ниже.



8. При необходимости установите отметку в поле "сохранить файл восстановления" и укажите путь для сохранения файла восстановления.

Внимание!

- Файл восстановления, который предлагается сохранить на данном этапе, теряет свою актуальность сразу при старте процесса шифрования. Рекомендуется создавать файл восстановления вручную после окончания процесса шифрования (см. стр.195, стр.197).
- Сохраните данные восстановления на диске, отличном от шифруемого.

9. Нажмите кнопку "Готово".

Начнется процесс шифрования. Появится окно с информацией о процессе.

Внимание! В процессе шифрования запрещается экстренная перезагрузка компьютера (нажатием кнопки Reset) или отключение шифруемого носителя информации во избежание повреждения и потери данных.

Пояснение.
- Для остановки процесса нажмите кнопку "Приостановить". Процесс шифрования будет приостановлен до нажатия кнопки "Запустить".
- Для отмены процесса нажмите кнопку "Отменить". Диск не будет зашифрован.
- В процессе шифрования допустима перезагрузка компьютера по команде из меню "Пуск" ОС Windows. После перезагрузки отобразится окно загрузчика Secret Net Studio, потребуется ввод пароля доступа к зашифрованным дискам. После входа в ОС процесс шифрования продолжится.

По окончании шифрования появится сообщение об этом. В мастере шифрования диску будет присвоен статус "Зашифрован". В Центре управления во вкладке "Общее" элемента "Полнодисковое шифрование" появится информация о зашифрованном разделе.

Локальное шифрование при централизованном хранении данных восстановления

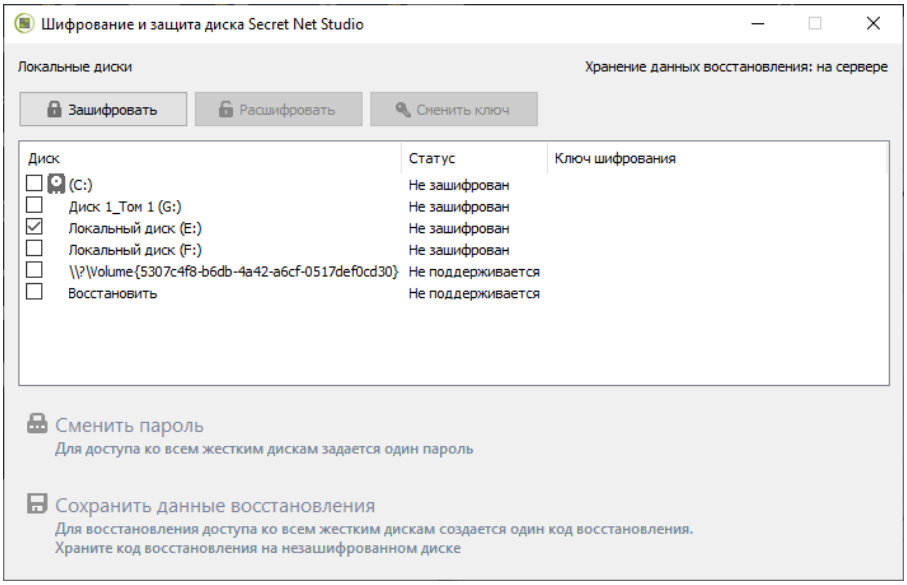
Для централизованного хранения данных восстановления необходимо активировать соответствующую настройку в Центре управления или в Локальном центре управления (см. стр.**182**).

Локальное шифрование выполняется с использованием мастера шифрования Secret Net Studio на компьютере, диски которого необходимо зашифровать. Пользователь, выполняющий шифрование, должен иметь привилегию на шифрование (см. стр.**182**).

Для шифрования:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Выберите команду "Шифрование".

   Появится окно мастера шифрования Secret Net Studio, подобное представленному на рисунке ниже.



Пояснение. Операцию шифрования можно запустить из контекстного меню диска. В пункте "Шифрование" выберите команду "Зашифровать" и перейдите к п. **4** данной инструкции.

2. Выберите диск, который необходимо зашифровать.

Пояснение.
- Имеется возможность шифрования нескольких дисков одновременно. Все диски компьютера шифруются с одним паролем доступа.
- Системный диск обозначается пиктограммой  .
- Диск со статусом "Не поддерживается" зашифровать нельзя. Требования к дискам, поддерживаемым подсистемой полнодискового шифрования, приведены на стр.182.

3. Нажмите кнопку "Зашифровать".

   Появится окно с запросом пароля доступа.

4. Установите пароль доступа к диску и подтверждение пароля или введите пароль к ранее зашифрованным дискам компьютера.

   Пояснение. Пароль доступа должен удовлетворять требованиям, указанным в окне запроса пароля.

   При необходимости установите отметку в поле "сменить пароль при первом доступе к зашифрованным дискам". В этом случае пользователь должен будет сменить пароль доступа при первой загрузке системы с зашифрованным диском.

5. Нажмите кнопку "Готово".

   Начнется процесс шифрования. Появится окно с информацией о процессе.

   Внимание! В процессе шифрования запрещается экстренная перезагрузка компьютера (нажатием кнопки Reset) или отключение шифруемого носителя информации во избежание повреждения и потери данных.

   Пояснение.
   - Для остановки процесса нажмите кнопку "Приостановить". Процесс шифрования будет приостановлен до нажатия кнопки "Запустить".
   - Для отмены процесса нажмите кнопку "Отменить". Диск не будет зашифрован.
   - В процессе шифрования допустима перезагрузка компьютера по команде из меню "Пуск" ОС Windows. После перезагрузки отобразится окно загрузчика Secret Net Studio, потребуется ввод пароля доступа к зашифрованным дискам. После входа в ОС процесс шифрования продолжится.

   По окончании шифрования появится сообщение об этом. В мастере шифрования диску будет присвоен статус "Зашифрован".

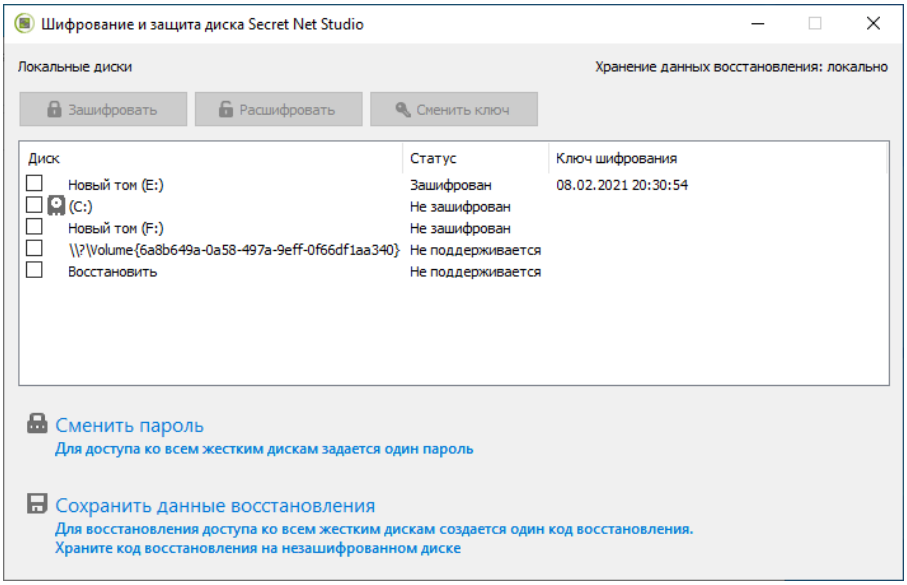
Локальное расшифрование

Локальное расшифрование выполняется с использованием мастера шифрования Secret Net Studio на компьютере, диски которого необходимо расшифровать. Пользователь, выполняющий расшифрование, должен иметь привилегию на шифрование (см. стр.182).

Для расшифрования:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Выберите команду "Шифрование".

   Появится окно мастера шифрования Secret Net Studio, подобное представленному на рисунке ниже.



Пояснение. Операцию расшифрования можно запустить из контекстного меню диска. В пункте "Шифрование" выберите команду "Расшифровать" и перейдите к п. **4** данной инструкции.

2. Выберите диск, который необходимо расшифровать.

Пояснение.
- Имеется возможность расшифрования нескольких дисков одновременно.
- Системный диск обозначается пиктограммой  .

3. Нажмите кнопку "Расшифровать".

   Появится окно с запросом пароля доступа.

4. Введите пароль доступа к диску.
5. Нажмите кнопку "Готово".

   Начнется процесс расшифрования. Появится окно с информацией о процессе.

Внимание! В процессе расшифрования запрещается экстренная перезагрузка компьютера (нажатием кнопки Reset) или отключение носителя информации во избежание повреждения и потери данных.

Пояснение.
- Для остановки процесса нажмите кнопку "Приостановить". Процесс расшифрования будет приостановлен до нажатия кнопки "Запустить".
- Для отмены процесса нажмите кнопку "Отменить". Диск не будет расшифрован.
- В процессе расшифрования допустима перезагрузка компьютера по команде из меню "Пуск" ОС Windows. После входа в ОС процесс расшифрования продолжится.

По окончании расшифрования появится сообщение об этом. В мастере шифрования диску будет присвоен статус "Не зашифрован".

Шифрование и расшифрование в Центре управления

Централизованное шифрование доступно для компьютеров с Secret Net Studio в автономном и сетевом режимах функционирования. При запуске на автономном компьютере будут зашифрованы диски этого компьютера. В сетевом режиме процедура может быть запущена для одного или нескольких компьютеров.

Процедура может быть выполнена при централизованном и локальном хранении данных восстановления.

Централизованное шифрование запускается администратором в Центре управления или в Локальном центре управления. Администратор, запускающий шифрование, должен иметь привилегию на шифрование (см. стр. **182**), а также на редактирование политик.

На компьютерах, для которых запущено шифрование, появляется уведомление об этом. В зависимости от режима хранения данных восстановления пользователю необходимо выполнить следующие действия:

- при централизованном хранении — указать пароль доступа к дискам;
- при локальном хранении — указать пароль доступа к дискам и параметры сохранения данных восстановления.

Пояснение. Подробные сведения о событиях на компьютере и действиях пользователя приведены в документе [3].

Для централизованного хранения данных восстановления необходимо активировать соответствующую настройку в Центре управления или в Локальном центре управления (см. стр.**182**).

Ниже приводится описание процедуры запуска централизованного шифрования в Центре управления. Локальный запуск выполняется аналогично в Локальном центре управления.

Для шифрования/расшифрования:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, на котором необходимо запустить централизованное шифрование. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки". В сетевом режиме функционирования загрузите параметры с сервера безопасности.

   Пояснение. Если выбран сервер безопасности, будет применена групповая политика и шифрование запустится на всех компьютерах с включенной подсистемой полнодискового шифрования, подчиненных этому серверу безопасности.

2. В разделе "Политики" перейдите к группе параметров "Полнодисковое шифрование".
3. Укажите действие для системных и несистемных разделов дисков компьютера, установив для параметров "Шифрование системных разделов" и/или "Шифрование несистемных разделов" одно из значений:
   - для шифрования — "Шифровать";
   - для расшифрования — "Не шифровать".

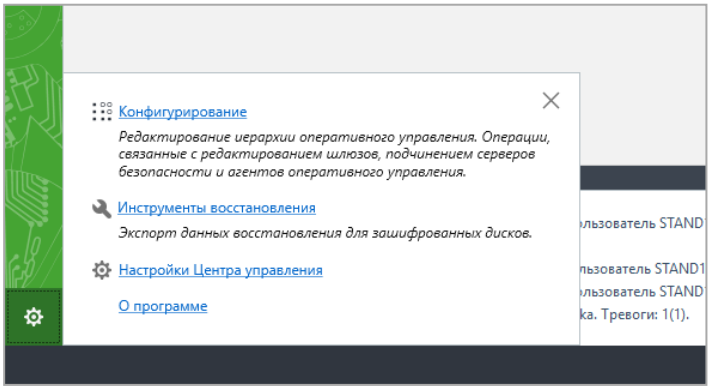
   Пояснение. При установке значения "Не шифровать" процесс расшифрования запустится после перезагрузки компьютера и монтирования зашифрованных дисков. Последующее шифрование дисков этого компьютера будет запрещено.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Смена ключа домена безопасности

Смена ключа домена безопасности выполняется администратором домена безопасности на сервере безопасности в Центре управления.

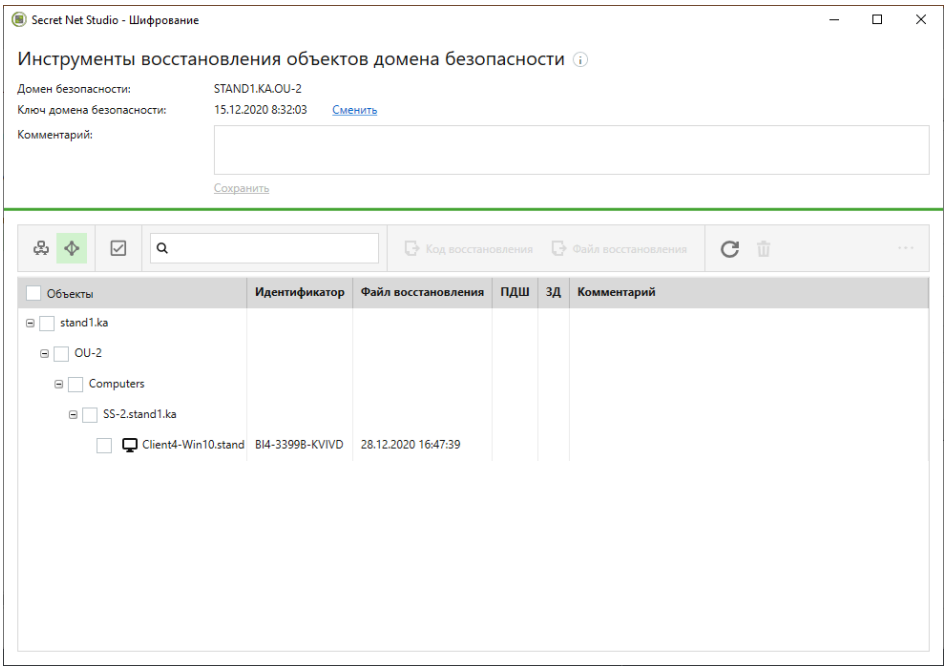
Для смены ключа домена безопасности:

1. В Центре управления в нижней части панели навигации нажмите кнопку "Настройки". На экране появится панель вызова средств настройки.



2. Выберите команду "Инструменты восстановления".

   Появится окно инструментов восстановления объектов домена безопасности, подобное представленному на рисунке ниже.



3. Нажмите кнопку "Сменить", расположенную рядом с информацией о ключе домена безопасности.

   Появится запрос пароля к ключу домена безопасности.

4. Введите пароль к ключу домена безопасности и нажмите кнопку "Далее".

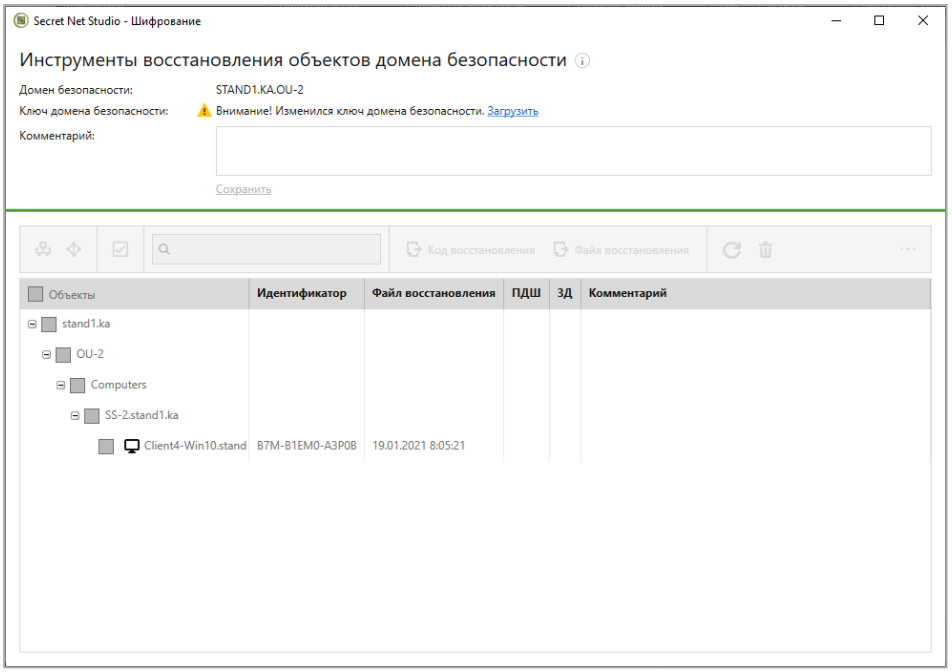
   Появится запрос на установку нового пароля.

5. Установите новый пароль к ключу домена безопасности и введите его повторно в поле "Подтверждение:".

   Пояснение. Пароль должен удовлетворять требованиям, указанным в окне запроса пароля.

6. Нажмите кнопку "Готово".

   В окне инструментов восстановления объектов домена безопасности появится уведомление о смене ключа. Операции с зашифрованными дисками станут недоступными для выполнения.



7. Нажмите кнопку "Загрузить".

   На компьютерах, которые подчинены данному серверу безопасности и на которых имеются зашифрованные диски, появится уведомление об изменении конфигурации системы защиты и необходимости перезагрузки.

   Операции с зашифрованными дисками в окне инструментов восстановления объектов домена безопасности станут доступными для выполнения.

Смена ключей шифрования

Смена ключей шифрования может быть выполнена:

- в Центре управления или Локальном центре управления;
- в мастере шифрования.

В Центре управления можно централизованно сменить ключи шифрования на компьютерах, подчиненных серверу безопасности, с локальным или централизованным хранением данных восстановления:

- при централизованном хранении в результате выполнения процедуры будет изменен код восстановления на сервере безопасности;
- при локальном хранении в результате выполнения процедуры пользователю отобразится уведомление о смене кода восстановления и необходимости сохранения новых данных восстановления.

Мастер шифрования позволяет сменить ключи шифрования локально для дисков компьютера. Такая смена ключей доступна только для компьютеров с локальным хранением данных восстановления. В результате смены ключей меняется код восстановления, необходимо сохранить новые данные восстановления.

Администратор, выполняющий смену ключей, должен иметь привилегию на шифрование (см. стр.182).

Ниже приводится описание процедур смены ключей шифрования в Центре управления и мастере шифрования. Смена ключей в Локальном центре управления выполняется аналогично процедуре смены в Центре управления.

Для смены ключей шифрования в Центре управления:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, на котором необходимо выполнить смену ключей. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Состояние" и выберите плитку "Полнодисковое шифрование".

Справа отобразится список дисков, для которых можно включить режим защиты.

Пояснение. Если выбран сервер безопасности, будет применена групповая политика и операция запустится на всех компьютерах с включенной подсистемой полнодискового шифрования, подчиненных этому серверу безопасности.

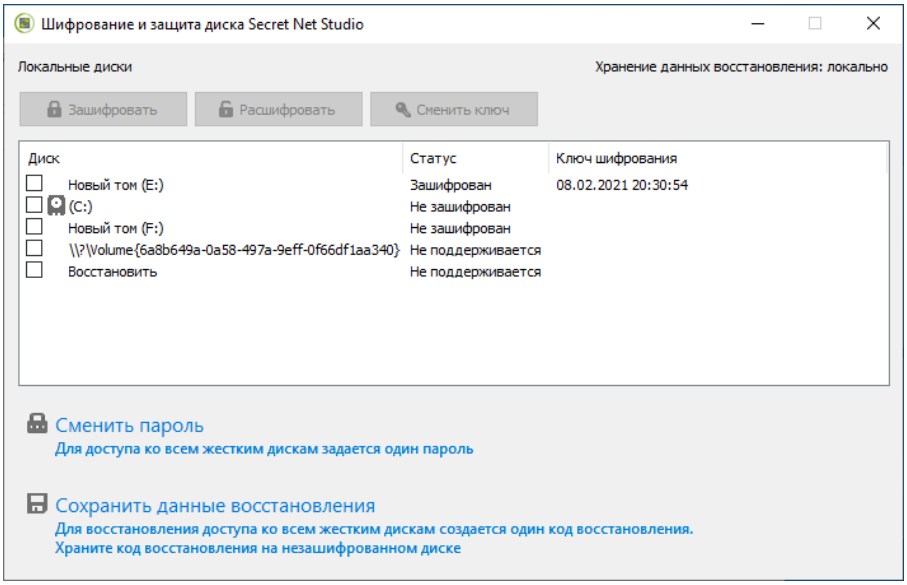
2. Выберите зашифрованные разделы, для которых необходимо сменить ключи.
3. Нажмите кнопку "Сменить ключ шифрования".

   Пользователям отобразится уведомление о необходимости перезагрузки компьютера. После перезагрузки запустится процесс смены ключей.

Для смены ключей шифрования в мастере шифрования:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Выберите команду "Шифрование".

   Появится окно мастера шифрования Secret Net Studio, подобное представленному на рисунке ниже.



Пояснение. Операцию смены ключей можно запустить из контекстного меню диска. В пункте "Шифрование" выберите команду "Сменить ключ шифрования" и перейдите к п. **4** данной инструкции.

2. Выберите зашифрованный диск, для которого необходимо сменить ключи шифрования.

Пояснение.

- Имеется возможность сменить ключи для нескольких зашифрованных дисков одновременно.
- Системный диск обозначается пиктограммой  .

3. Нажмите кнопку "Сменить ключ".

   Появится окно с запросом пароля доступа.

4. Введите пароль доступа к зашифрованным дискам компьютера и нажмите кнопку "Готово".

   Запустится процесс расшифрования данных для смены ключа.

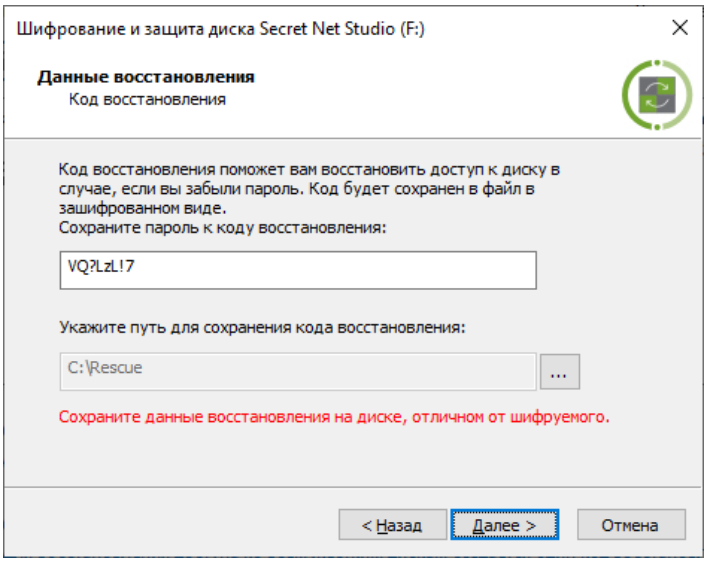
Внимание! В процессе расшифрования запрещается экстренная перезагрузка компьютера (нажатием кнопки Reset) или отключение носителя информации во избежание повреждения и потери данных.

Пояснение. В процессе расшифрования допустима перезагрузка компьютера по команде из меню "Пуск" ОС Windows. После входа в ОС процесс продолжится.

По завершении процесса появится запрос пароля доступа к зашифрованным дискам для сохранения новых данных восстановления.

5. Введите пароль доступа к зашифрованным дискам и нажмите кнопку "Далее".

   Появится окно сохранения кода восстановления, подобное представленному на рисунке ниже.



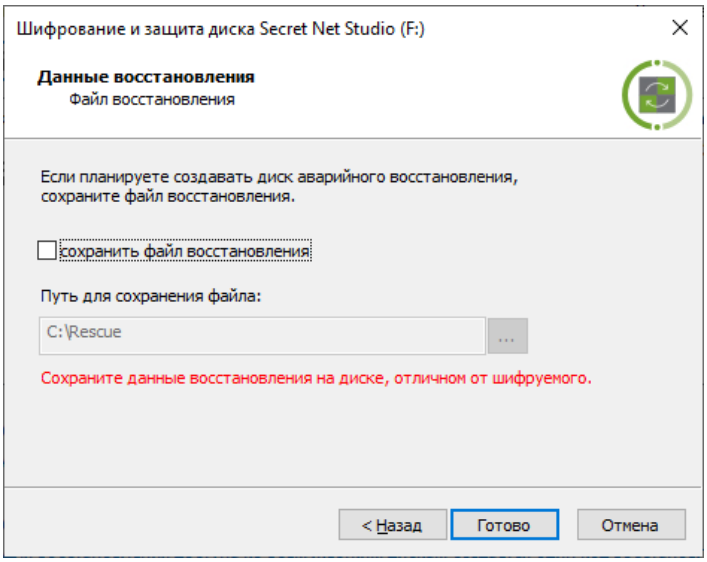
6. Сохраните пароль к коду восстановления, сгенерированный системой. Укажите путь для сохранения кода восстановления.

   Внимание! Сохраните данные восстановления на диске, отличном от шифруемого.

   Пояснение. Код восстановления можно сохранить повторно позже (см. стр.195).

7. Нажмите кнопку "Далее".

   Появится окно сохранения файла восстановления, подобное представленному на рисунке ниже.



8. При необходимости создания диска аварийного восстановления установите отметку в поле "сохранить файл восстановления" и укажите путь для сохранения файла восстановления.

   Внимание! Сохраните данные восстановления на диске, отличном от шифруемого.

9. Нажмите кнопку "Готово".

   Запустится процесс шифрования на новом ключе.

Внимание! В процессе шифрования запрещается экстренная перезагрузка компьютера (нажатием кнопки Reset) или отключение носителя информации во избежание повреждения и потери данных.

Пояснение. В процессе шифрования допустима перезагрузка компьютера по команде из меню "Пуск" ОС Windows. После входа в ОС процесс продолжится.

Восстановление доступа к зашифрованным дискам

Подсистема полнодискового шифрования Secret Net Studio предоставляет следующие возможности восстановления данных на зашифрованных дисках:

- **В случае утери пароля доступа к дискам** можно восстановить доступ с помощью кода восстановления, пароля к коду восстановления и идентификатора зашифрованного диска (см. стр.**199**).

  Идентификатор зашифрованного диска и код восстановления сохраняются в файл. При локальном хранении данных восстановления файл создается и хранится локально на компьютере, на котором выполняется шифрование (см. стр.**195**). При централизованном хранении данных восстановления файл необходимо экспортировать на сервере безопасности (см. стр.**197**).

  Пароль к коду восстановления генерируется автоматически при каждой процедуре сохранения или экспорта кода восстановления. Код восстановления шифруется на этом пароле. Пароль к коду восстановления необходимо хранить в надежном месте и передавать только по защищенному каналу.

  Восстановление доступа выполняется администратором в загрузчике Secret Net Studio.

- **В случае повреждения зашифрованного диска или затирания служебной информации** можно расшифровать диск, восстановить загрузчик Secret Net Studio или восстановить конфигурацию подсистемы полнодискового шифрования с помощью диска аварийного восстановления (см. стр.**299**). При создании диска, который будет использоваться для расшифрования и восстановления конфигурации, понадобится файл восстановления.

  При локальном хранении данных восстановления файл восстановления создается и хранится локально на компьютере, на котором выполняется шифрование (см. стр. **195**). При централизованном хранении данных восстановления файл восстановления необходимо экспортировать на сервере безопасности (см. стр.**197**).

Внимание! При использовании подсистемы полнодискового шифрования настоятельно рекомендуется создавать диск аварийного восстановления с актуальным файлом восстановления. Так, если при зашифрованном системном диске вышел из строя загрузчик Secret Net Studio, то ОС не будет загружаться, и исправить проблему можно только с помощью диска аварийного восстановления.
Файл восстановления, который предлагается сохранить в мастере шифрования на этапе шифрования, теряет свою актуальность сразу при старте процесса шифрования. Рекомендуется создавать файл восстановления вручную после окончания процесса шифрования (см. стр.**195**, стр.**197**).

Пояснение. Перечень других возможностей диска аварийного восстановления приведен на стр.**299**.

Локальное сохранение данных восстановления

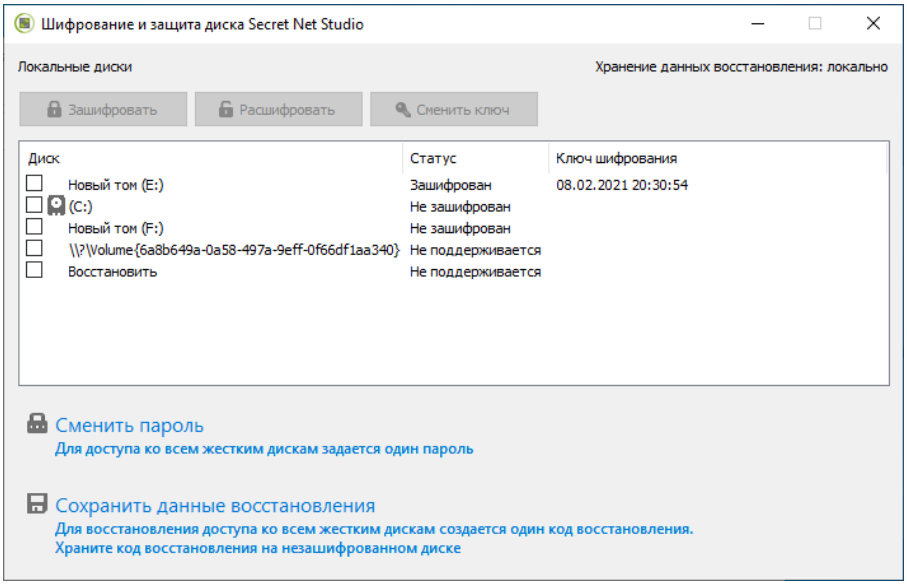
Если данные восстановления не были сохранены при шифровании данных на дисках, их можно сохранить позже в мастере шифрования Secret Net Studio. Данная операция доступна только при локальном хранении данных восстановления.

Администратор, сохраняющий данные восстановления, должен иметь привилегию на шифрование (см. стр.**182**).

Для сохранения данных восстановления:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows. Выберите команду "Шифрование".

   Появится окно мастера шифрования Secret Net Studio, подобное представленному на рисунке ниже.



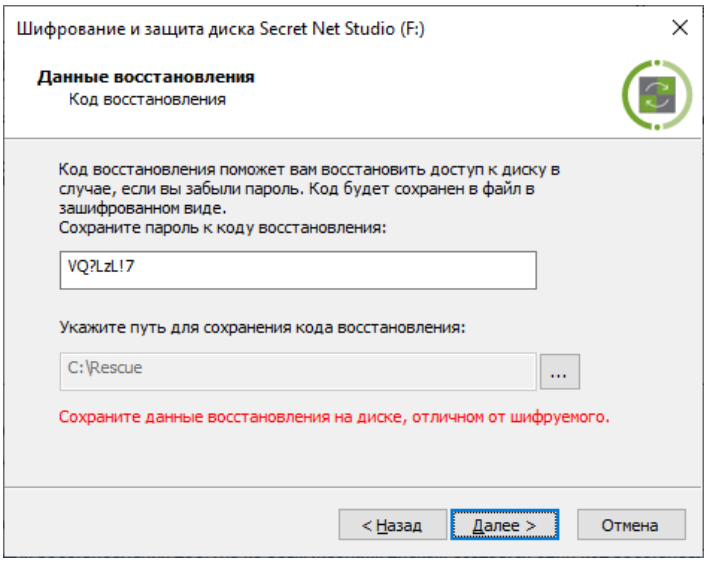
Пояснение. Операцию можно запустить из контекстного меню диска. В пункте "Шифрование" выберите команду "Сохранить данные восстановления" и перейдите к п. **3** данной инструкции.

2. Нажмите кнопку "Сохранить данные восстановления".

   Появится окно с запросом пароля доступа.

3. Введите пароль к зашифрованным дискам компьютера и нажмите кнопку "Далее".

   Появится окно сохранения кода восстановления, подобное представленному на рисунке ниже.

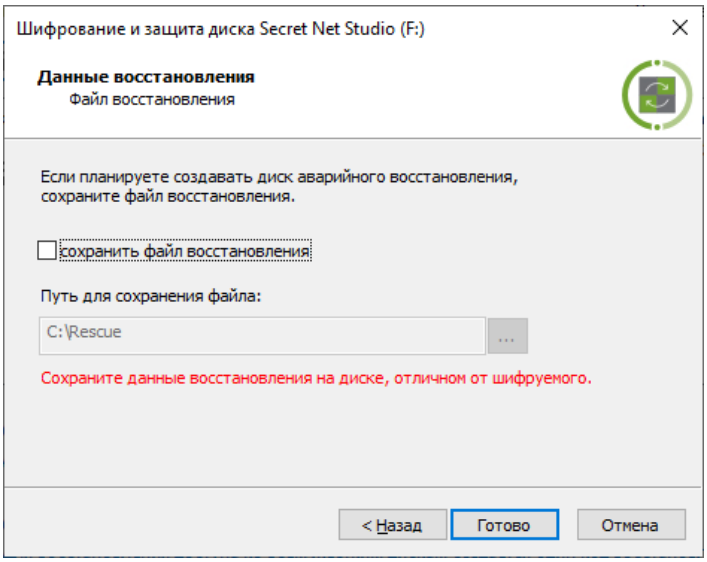


4. Сохраните пароль к коду восстановления, сгенерированный системой. Укажите путь для сохранения кода восстановления.

Внимание! Сохраните данные восстановления на диске, отличном от шифруемого.

5. Нажмите кнопку "Далее".

Появится окно сохранения файла восстановления, подобное представленному на рисунке ниже.



6. При необходимости установите отметку в поле "сохранить файл восстановления" и укажите путь для сохранения файла восстановления.

Внимание! Сохраните данные восстановления на диске, отличном от шифруемого.

7. Нажмите кнопку "Готово".

Отобразится уведомление об успешном сохранении данных восстановления.

Экспорт данных восстановления на сервере безопасности

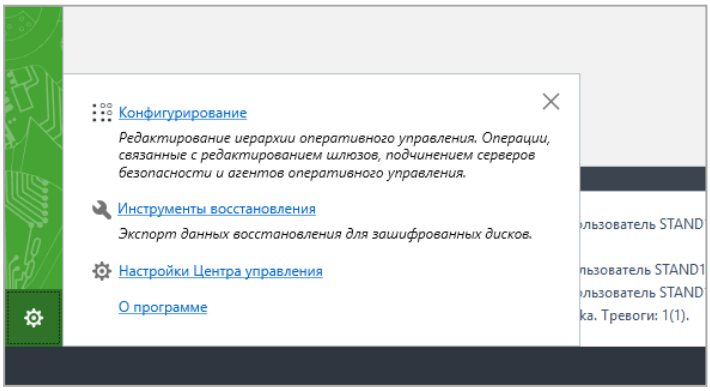
При централизованном хранении данных восстановления необходимо экспортировать эти данные на сервере безопасности и передать пользователю. Код и файл восстановления могут быть переданы по открытому каналу связи. Пароль к коду восстановления необходимо передавать только по защищенному каналу связи.

Экспорт кода и файла восстановления выполняется администратором в Центре управления.

Администратор, выполняющий экспорт, должен иметь привилегию на шифрование (см. стр.**182**).

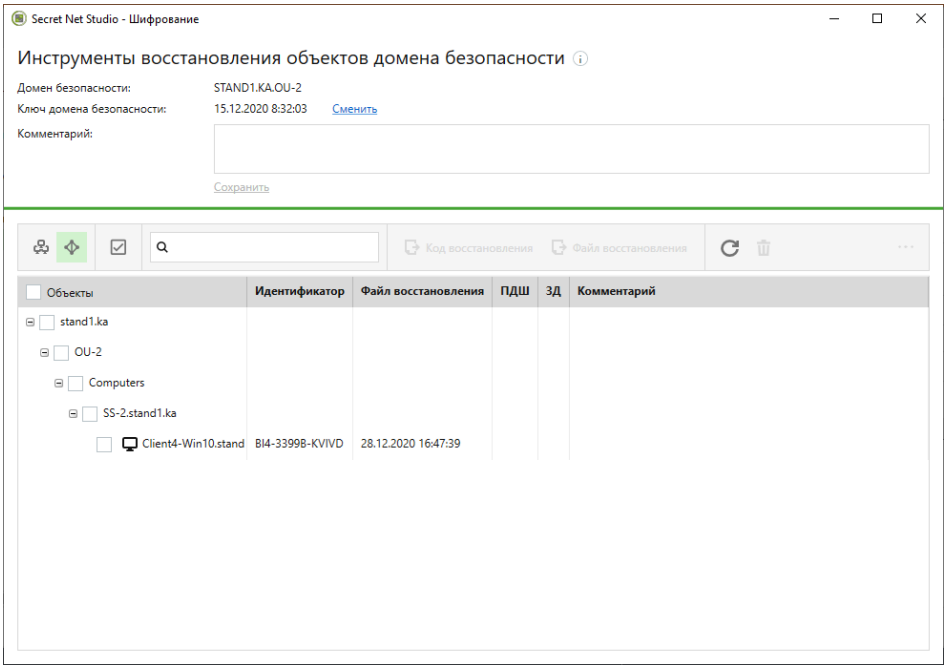
Для экспорта кода восстановления:

1. В Центре управления в нижней части панели навигации нажмите кнопку "Настройки". На экране появится панель вызова средств настройки.



2. Выберите команду "Инструменты восстановления".

Появится окно инструментов восстановления объектов домена безопасности, подобное представленному на рисунке ниже.



3. Выберите объект, для которого необходимо экспортировать код восстановления.

Пояснение.

- Объекты могут быть представлены в виде структуры объекта управления и структуры AD. Для выбора режима отображения объектов нажмите кнопки  и  соответственно.
- Можно выбрать несколько объектов.
- При выборе компьютера код восстановления для всех зашифрованных дисков этого компьютера экспортируется в один файл.
- При выборе сервера безопасности или нескольких компьютеров коды восстановления для каждого компьютера экспортируются в отдельные файлы.

4. Нажмите кнопку "Экспортировать код восстановления".

   Появится запрос пароля к ключу домена безопасности.

5. Введите пароль к ключу домена безопасности и нажмите кнопку "Далее".

   Появится окно указания пути для сохранения.

6. Укажите путь для сохранения кода восстановления и нажмите кнопку "Готово".

   Появится окно с паролем к коду восстановления, который сгенерирован системой защиты.

7. Сохраните пароль к коду восстановления для передачи его пользователю по защищенному каналу. Нажмите кнопку "Готово".

Для экспорта файла восстановления:

1. В Центре управления в нижней части панели навигации нажмите кнопку "Настройки". На экране появится панель вызова средств настройки (см. рисунок в п. 1 инструкции выше).
2. Выберите команду "Инструменты восстановления".

   Появится окно инструментов восстановления объектов домена безопасности (см. рисунок в п. 2 инструкции выше).

3. Выберите объект, для которого необходимо экспортировать файл восстановления.

Пояснение.

- Объекты могут быть представлены в виде структуры объекта управления и структуры AD. Для выбора режима отображения объектов нажмите кнопки  и  соответственно.
- Можно выбрать несколько объектов.
- При выборе компьютера экспортируется один файл восстановления для всех зашифрованных дисков этого компьютера.
- При выборе сервера безопасности или нескольких компьютеров экспортируются файлы восстановления для каждого объекта отдельно.

4. Нажмите кнопку "Экспортировать файл восстановления".

   Появится запрос пароля к ключу домена безопасности.

5. Введите пароль к ключу домена безопасности нажмите кнопку "Далее".

   Появится окно указания пути для сохранения.

6. Укажите путь для сохранения файла восстановления и нажмите кнопку "Готово".

Восстановление доступа с помощью кода восстановления

Восстановление доступа к зашифрованным дискам выполняется администратором в загрузчике Secret Net Studio. Администратор должен иметь файл с кодом восстановления и идентификатором зашифрованного диска, а также знать пароль к коду восстановления.

При успешном восстановлении доступа выполняется смена пароля доступа к дискам, идентификатора зашифрованных дисков, кода восстановления и пароля к нему. При этом:

- при централизованном хранении данных восстановления эти данные обновляются на сервере безопасности при монтировании зашифрованных дисков;
- при локальном хранении данных восстановления система выведет пользователю запрос на сохранение новых данных.

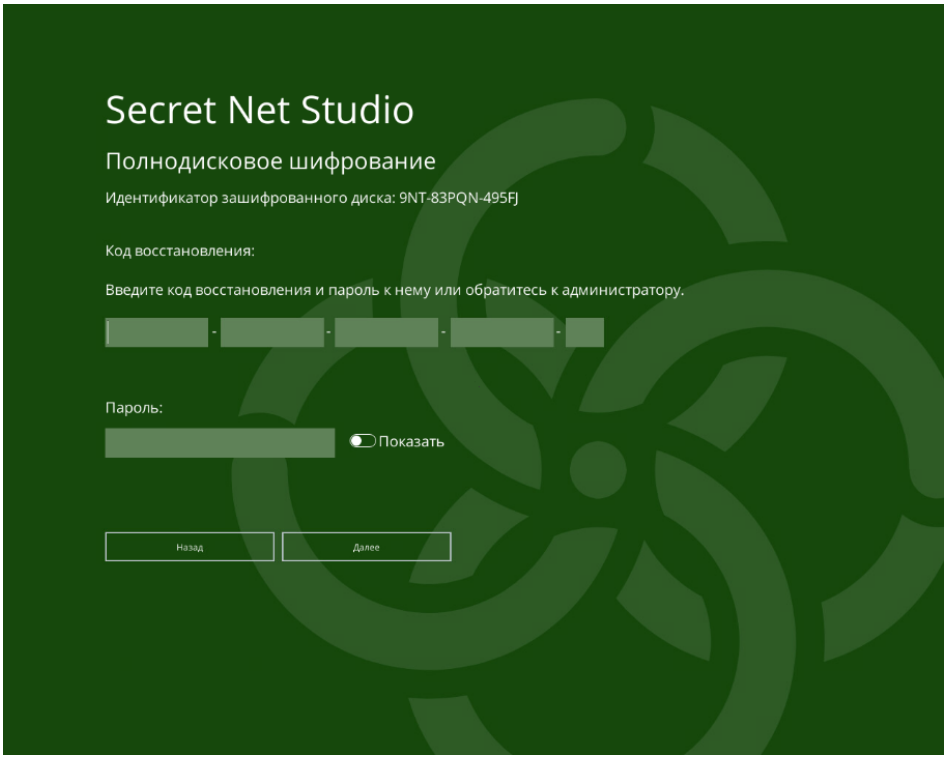
Для восстановления доступа:

1. Включите компьютер.

   Появится окно загрузчика Secret Net Studio.

2. Выберите команду "Восстановление доступа".

   Появится окно с запросом данных восстановления, подобное представленному на рисунке ниже.



3. Сравните идентификатор зашифрованного диска с идентификатором из файла с кодом восстановления. Они должны совпадать.

   Пояснение. Если идентификаторы не совпадают, то данные из файла не подойдут для восстановления доступа к дискам на данном компьютере.

4. Введите код восстановления и пароль к нему.
5. Нажмите кнопку "Далее".

   При вводе корректных данных доступ к дискам будет восстановлен. Появится окно установки нового пароля доступа.
6. Установите новый пароль доступа к дискам. Введите подтверждение пароля.
7. Нажмите кнопку "Далее".

   Выполнится загрузка ОС. При централизованном хранении данных восстановления на сервере безопасности будут обновлены данные восстановления. При локальном хранении данных восстановления при входе пользователя в ОС появится запрос пароля доступа к дискам для сохранения новых данных восстановления.

   Пояснение. Подробные сведения о событиях на компьютере и действиях пользователя при локальном хранении данных восстановления приведены в документе [3].

Глава 15
Шифрование данных в криптоконтейнерах

Предоставление привилегии для создания криптоконтейнеров

В механизме шифрования данных в криптоконтейнерах создание криптоконтейнеров доступно пользователям, которым предоставлена привилегия "Создание криптоконтейнера".

По умолчанию привилегией на создание криптоконтейнеров обладают пользователи, входящие в локальную группу администраторов и в группу "Пользователи".

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для предоставления привилегии:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Защита диска и шифрование данных".
3. Для параметра "Учетные записи с привилегией на создание криптоконтейнера" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма шифрования данных в криптоконтейнерах, необходимо выполнить настройку регистрации событий. Настройка выполняется в Центре управления.

События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Защита диска и шифрование данных". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. выше) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

Управление криптографическими ключами пользователей

Для работы с зашифрованными данными в криптоконтейнерах пользователям необходимо загружать криптографические ключи (ключевую информацию) со своих ключевых носителей. Ключевая информация может храниться в присвоенном пользователю персональном идентификаторе или сменном носителе.

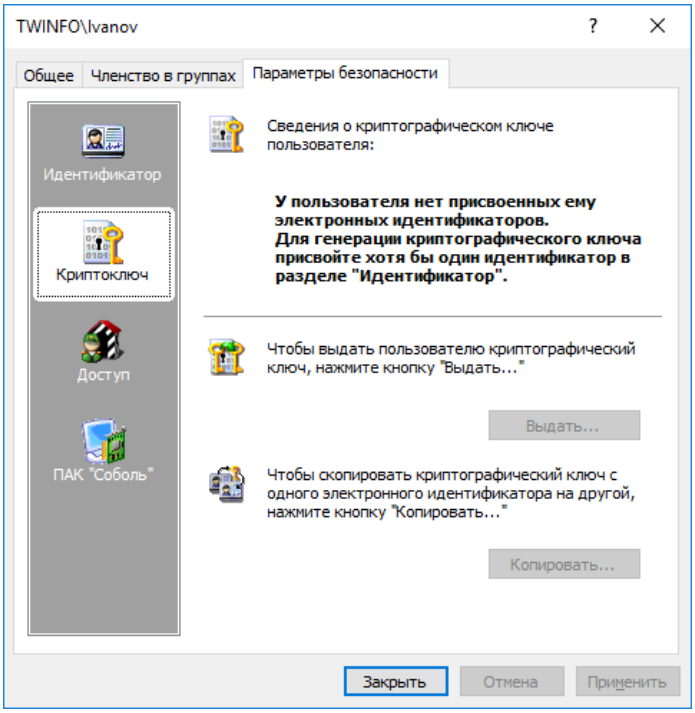
Выдача и смена ключей

Генерация ключевой информации и запись закрытого ключа на ключевой носитель может выполняться при присвоении пользователю персонального идентификатора. Описание процедуры присвоения см. на стр.31. Если пользователю присвоен идентификатор, но ключевая информация не была сгенерирована или требуется сменить имеющиеся ключи, администратор может выполнить процедуру выдачи/смены ключей.

Для выдачи/смены ключей:

1. Запустите программу управления пользователями (обзор программы приведен на стр.**270**).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. В панели выбора групп параметров выберите группу "Криптоключ".

   В диалоге будут отображены сведения о ключах пользователя.



4. Нажмите кнопку "Выдать" (если у пользователя уже есть ключи, эта кнопка называется "Сменить"). Кнопка активна, если пользователю присвоен хотя бы один идентификатор.

   Если пользователь уже имеет ключи, на экране появится диалог, предлагающий выбрать один из двух вариантов смены ключей — с сохранением старого ключа пользователя или без его сохранения.
5. Выберите нужный вариант и нажмите кнопку "Далее >".

> **Внимание!** Вариант без сохранения рекомендуется использовать только в тех случаях, когда невозможно считать текущий ключ с идентификаторов пользователя. Для подтверждения выбора введите в текстовое поле слово "продолжить" (без кавычек) и нажмите кнопку "Далее >". В этом случае программа перейдет к шагу "Запись ключей".

   Если был выбран вариант с сохранением старого ключа, на экране появится диалог, отображающий ход выполнения операции чтения ключа, и приглашение предъявить идентификатор.
6. Предъявите идентификатор, содержащий старый закрытый ключ данного пользователя.

   После успешного выполнения операции в диалоге справа от названия операции появится запись "Выполнено". Если при выполнении операции возникла ошибка, в диалоге будет приведено сообщение об этом.

> **Примечание.** Продолжение процедуры без устранения ошибки невозможно.

7. Если возникла ошибка, нажмите кнопку "Повторить" для повторного выполнения операции. После устранения ошибки нажмите кнопку "Далее >".

   На экране появится диалог, отображающий ход выполнения операций, и приглашение предъявить идентификаторы.
8. Предъявите все идентификаторы, указанные в списке.

При успешном предъявлении идентификатора его статус изменится на "Обработан". Если предъявление идентификатора выполнено с ошибкой, в столбце статуса обработки появится сообщение об ошибке. После предъявления всех идентификаторов кнопка "Отмена" будет заменена кнопкой "Закрыть".

9. Нажмите кнопку "Закрыть".

   На экране появится диалог с результатами выполнения операций. Если операции выполнены с ошибками, в диалоге будет приведено их описание.

10. Устраните ошибки, если они возникли. Для этого нажмите кнопку "< Назад" и повторно выполните операцию. После устранения ошибок нажмите кнопку "Готово".

Внимание! Настоятельно рекомендуется исправлять ошибки, произошедшие при записи ключей в идентификаторы. После успешного завершения всех предусмотренных операций для каждой из них должно быть указано состояние "Выполнено".

Копирование ключей

Ключи пользователя, сгенерированные средствами системы Secret Net Studio, можно скопировать с одного идентификатора пользователя на другой. Процедура копирования выполняется администратором безопасности.

Для копирования ключей:

1. Запустите программу управления пользователями (обзор программы приведен на стр.**270**).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. В панели выбора групп параметров выберите группу "Криптоключ".
4. Нажмите кнопку "Копировать". Кнопка активна, если пользователю присвоены хотя бы два идентификатора.

   На экране появится диалог "Предъявите идентификатор".

5. Предъявите идентификатор, содержащий копируемые ключи пользователя.

   Произойдет считывание ключей, и на экране появится диалог со списком идентификаторов пользователя.

6. Предъявите идентификатор, на который требуется записать ключи.

   При успешной записи ключей в идентификатор его статус изменится на "Обработан".

7. Нажмите кнопку "Закрыть".

Настройка параметров смены ключей

Администратор может настраивать следующие параметры смены ключей, сгенерированных средствами системы Secret Net Studio:

- максимальный срок действия;
- минимальный срок действия;
- время предупреждения об истечении срока действия ключа.

Действие параметров распространяется на всех пользователей. По истечении максимального срока действия ключевая информация пользователя становится недействительной. В этом случае пользователь должен сменить ключевую информацию (см. раздел "Смена ключевой информации" документа [**3**]). Смена ключевой информации самим пользователем возможна только по истечении минимального срока действия ключа.

Данные параметры взаимосвязаны. Минимальный срок действия и время предупреждения об истечении срока действия не могут быть равны или превышать максимальный срок действия ключа.

Ниже приводится описание процедуры централизованной настройки при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки параметров:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Ключи пользователя".
3. Укажите нужные значения для параметров "Максимальный срок действия ключа", "Минимальный срок действия ключа" и "Предупреждение об истечении срока действия ключа".

   Примечание. Если установлено нулевое значение, параметр не применяется.

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Глава 14
Затирание удаляемой информации

Подсистема затирания данных в Secret Net Studio предназначена для затирания областей памяти, в которых остаются данные от удаленных объектов. Это предотвращает возможность восстановления данных после удаления и обеспечивает безопасность повторного использования носителей информации. Затирание может выполняться:

- автоматически на устройствах определенных типов (локальные и сменные диски, оперативная память) при включении функции затирания в Центре управления;

  Примечание. Имеется возможность исключать выбранные объекты (файлы и папки) из обработки при автоматическом затирании (см. стр.**206**).

- по команде из контекстного меню для файловых объектов, выбранных пользователем;
- по команде из контекстного меню пиктограммы Secret Net Studio в панели задач Windows на локальных дисках (кроме системного диска) и сменных носителях, подключенных к защищаемому компьютеру.

Внимание! Затирание файла подкачки виртуальной памяти выполняется стандартными средствами ОС Windows при выключении компьютера. Если в Secret Net Studio включен режим затирания оперативной памяти, рекомендуется дополнительно включить действие стандартного параметра безопасности Windows "Завершение работы: очистка файла подкачки виртуальной памяти".
Не осуществляется затирание файлов при их перемещении в папку "Корзина", так как во время нахождения в этой папке файлы не удаляются с диска. Затирание таких файлов происходит после очистки содержимого "Корзины".

Данная глава содержит описание следующих процедур:

- настройка механизма затирания (стр.**205**);
- настройка списка исключения для автоматического затирания (стр.**206**);
- отслеживание процесса отложенного затирания остаточных данных (стр.**207**);
- уничтожение данных на носителях информации (стр.**208**).

Настройка механизма затирания

Ниже приводится описание процедуры централизованной настройки механизма затирания при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки механизма:

1. В Центре управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Затирание данных".
3. Укажите нужные значения для параметров затирания:
   - "Количество циклов затирания на локальных дисках";
   - "Количество циклов затирания на сменных носителях";
   - "Количество циклов затирания оперативной памяти";
   - "Количество циклов затирания по команде "Удалить безвозвратно";
   - "Количество циклов затирания при уничтожении данных на дисках".

Примечание. Если параметру присвоено значение "0", затирание не выполняется. Для гарантированного уничтожения данных в большинстве случаев достаточно двух проходов затирания.

Совет. Для просмотра справочной информации о параметре нажмите кнопку .

4. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Список исключений

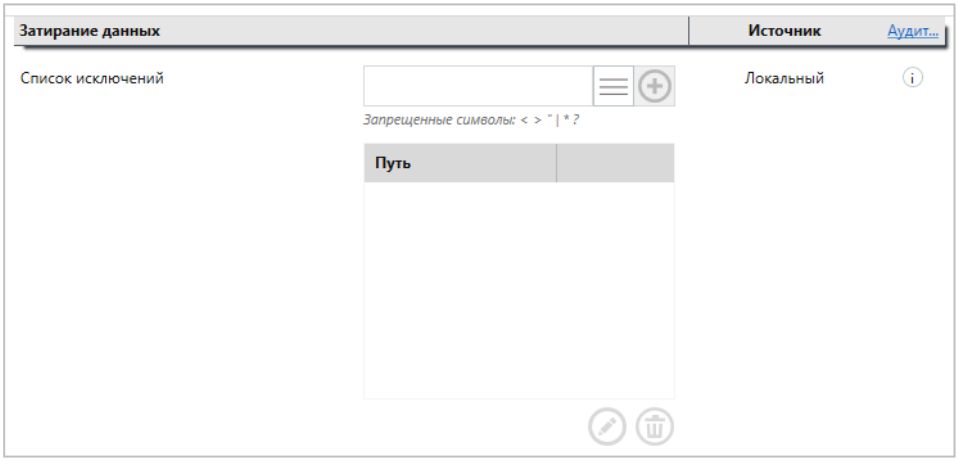
Функция предназначена для исключения выбранных объектов (файлов и папок) из обработки при автоматическом затирании данных на локальных дисках и сменных носителях.

Примечание.
- При добавлении папки в список исключений все объекты этой папки будут пропускаться при автоматическом затирании данных.
- Список исключений можно создать и для локальной, и для групповой политики.

Ниже приводится описание процедуры централизованной настройки списка исключений при работе с Центром управления. Локальная настройка выполняется аналогично с использованием Локального центра управления.

Для настройки списка исключений:

1. В области настройки механизма затирания данных перейдите к параметру "Список исключений":



2. Выполните необходимое действие:
   - для добавления объекта в список исключений укажите полный путь к объекту и нажмите кнопку . При необходимости используйте переменные среды окружения из раскрывающегося списка, нажав кнопку ;
   - для изменения пути к объекту выберите его в списке исключений и нажмите кнопку ;
   - для удаления объекта из списка исключений нажмите кнопку .
3. Для сохранения изменений нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Примечание. Для отмены изменений нажмите кнопку "Отменить".

Отложенное затирание остаточных данных

Механизм отложенного затирания предназначен для снижения нагрузки на компьютер при удалении большого объема данных с локальных дисков и сменных носителей. Остаточные данные, подлежащие затиранию, добавляются в очередь на обработку. Затирание выполняется в порядке очереди, с временной задержкой, и завершается до выключения компьютера.

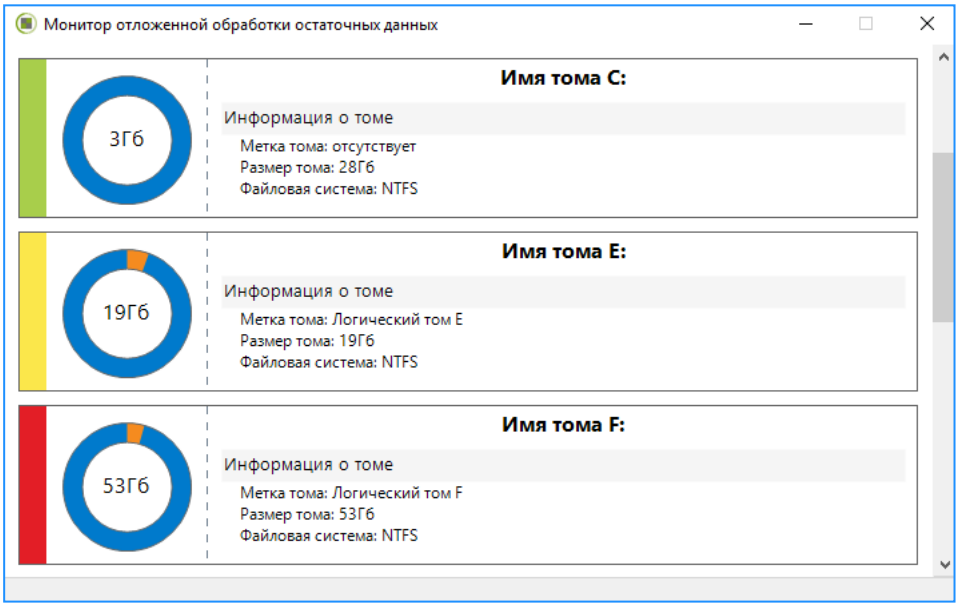
Процесс отложенного затирания можно отследить на мониторе отложенной обработки остаточных данных.

Внимание! Монитор отложенной обработки остаточных данных доступен при включенной подсистеме затирания данных и количестве циклов затирания на локальных дисках или сменных носителях больше "0" (см. стр.205).

Для просмотра монитора:

- Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows и выберите команду "Удаление данных | Монитор отложенной обработки остаточных данных".

  Появится окно, подобное следующему:



Монитор отображает информационные панели для каждого логического тома, на котором выполняется отложенное затирание.

Информационная панель содержит следующие сведения:

- имя логического тома или точка монтирования;
- информация о логическом томе (метка тома, размер тома, файловая система);
- вертикальный цветовой индикатор отображает временную задержку на обработку затираемых остаточных данных с учетом количества циклов затирания:
  - зеленый — время на обработку менее 10 секунд;
  - желтый — время на обработку от 10 до 60 секунд;
  - красный — время на обработку более 60 секунд;
  - серый — выполняется оценка требуемого времени;
- круговая диаграмма отображает отношение объема свободного пространства тома к объему затираемых остаточных данных без учета количества циклов затирания:
  - голубой — объем свободного пространства логического тома;
  - оранжевый — объем затираемых остаточных данных.

Уничтожение данных на носителях информации

Функция предназначена для безвозвратного затирания всей информации (включая таблицу разделов, логические тома, файловые объекты и остаточную информацию) на следующих носителях информации:

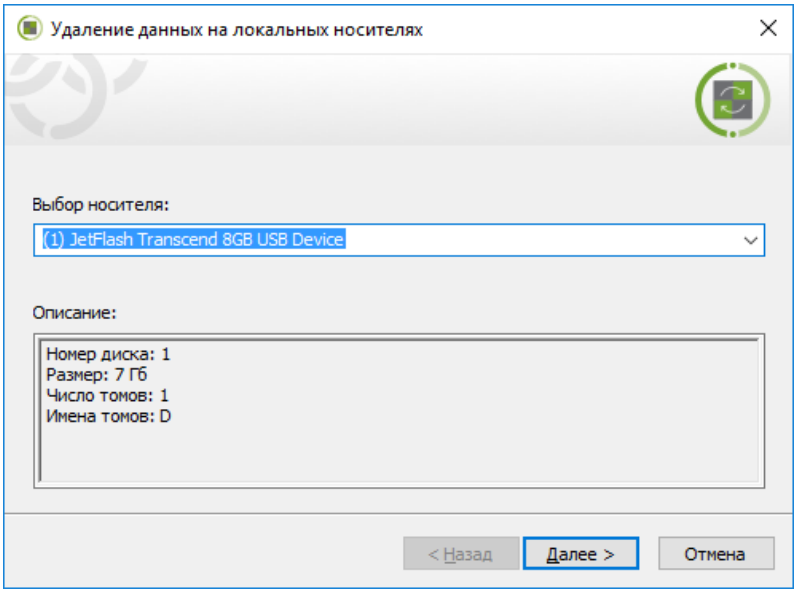
- локальные диски защищаемого компьютера (кроме системного диска);
- сменные носители информации, подключенные к защищаемому компьютеру.

Внимание! Функция уничтожения данных на носителях информации доступна только пользователям, входящим в локальную группу администраторов компьютера.

Для уничтожения данных на носителе информации:

1. Вызовите контекстное меню пиктограммы Secret Net Studio в системной области панели задач Windows и выберите команду "Удаление данных | Удаление данных на локальных носителях".

   Появится диалог выбора носителя информации:



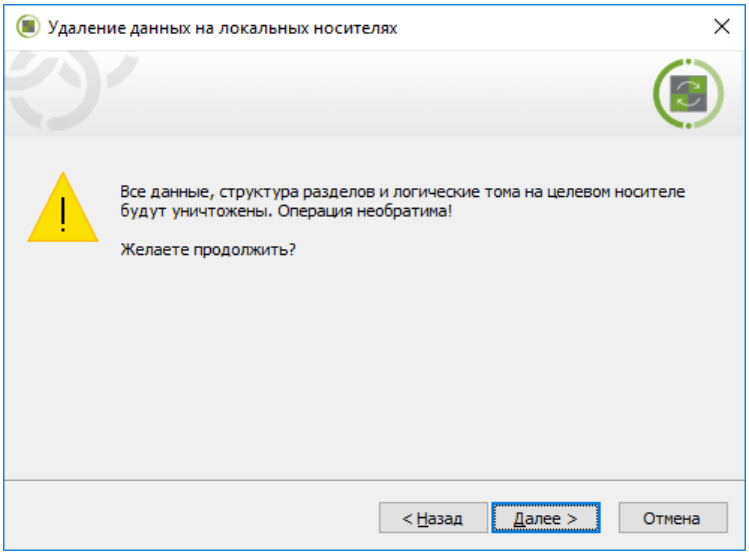
2. Выберите в раскрывающемся списке носитель, на котором необходимо уничтожить данные.

   Пояснение. Если съемные носители не подключены и на компьютере имеется только системный локальный диск, список носителей будет пуст.

   В поле "Описание" появятся сведения о носителе.

3. Нажмите кнопку "Далее >".

   Появится запрос на продолжение операции уничтожения данных.



4. Если вы уверены, что хотите безвозвратно уничтожить все данные на носителе, нажмите "Далее >".

   Начнется процесс затирания информации.

   Пояснение. Процесс затирания может занять длительное время. Длительность зависит от количества циклов затирания, установленных в программе управления (параметр "Количество циклов затирания при уничтожении данных на дисках"), и объема носителя.

   По окончании процесса появится сообщение об успешном его завершении.

5. Нажмите кнопку "Готово".

Глава 15
Персональный межсетевой экран

Персональный межсетевой экран предназначен для защиты серверов и рабочих станций локальной сети от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

Механизм защиты обеспечивает фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях. Фильтрация трафика осуществляется на основе формируемых для приложений правил.

Персональный межсетевой экран выполняет следующие функции.

Функция	Описание
Фильтрация сетевого трафика	Для фильтрации сетевого трафика используются специальные правила, обладающие широким диапазоном настроек. Сетевые соединения можно ограничивать на следующих уровнях: • пользователи; • компьютеры; • группы пользователей (компьютеров); • параметры соединения — служебные и прикладные протоколы, порты, сетевые интерфейсы, приложения, дни недели, время суток
Режим обучения	При включенном режиме обучения разрешается весь сетевой трафик. Для каждого пакета проверяется наличие правила фильтрации (правила с реакцией "по умолчанию" не проверяются). Если правила нет, оно добавляется как разрешающее для каждого из приложений. Однотипные правила заменяются одним правилом, включающим в себя все объединенные

Настройка межсетевого экрана осуществляется централизованно в Центре управления. Она выполняется на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров.

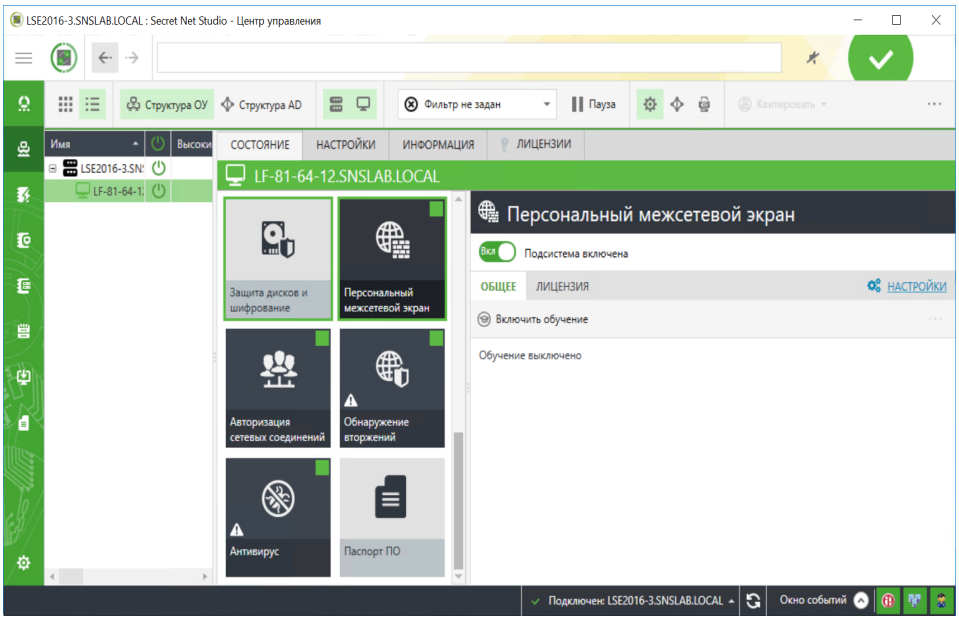
Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". С помощью данного компонента можно только посмотреть настройки механизма межсетевого экрана непосредственно на защищаемом компьютере.

После установки Secret Net Studio на защищаемом компьютере первоначальная настройка межсетевого экрана разрешает прохождение всего сетевого трафика.

Для настройки межсетевого экрана:

1. Откройте Центр управления Secret Net Studio.

На экране появится основное окно программы.



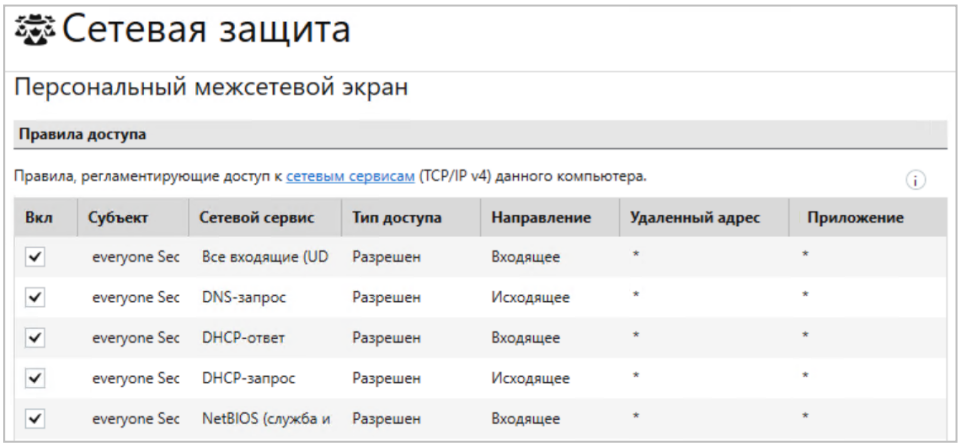
Совет. Для просмотра значений параметров межсетевого экрана непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Персональный межсетевой экран". В локальном режиме управления редактирование параметров недоступно.

2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

   В правой части экрана появится информация о состоянии компьютера.

3. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Персональный межсетевой экран".

   В правой части экрана появится область настройки выбранных параметров.



4. Настройте нужные параметры и для сохранения новых значений нажмите кнопку "Применить" внизу вкладки "Настройки".

Внимание! Если для двух защищаемых компьютеров выбраны разные режимы аутентификации (см. стр.12), правила межсетевого экрана для аутентифицированных пользователей между ними не сработают.

Порядок обработки сетевых пакетов

Порядок обработки пакетов в Secret Net Studio зависит от направления сетевого трафика.

- Входящие пакеты — первоначально выполняется проверка на соответствие настройкам сетевых протоколов, затем — на соответствие системным правилам, а затем, если пакет пропущен, — на соответствие правилам доступа.
- Исходящие пакеты — сначала выполняется проверка на соответствие правилам доступа, затем — на соответствие системным правилам, а затем, если пакет пропущен, — на соответствие настройкам сетевых протоколов.

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы (см. стр.212).

При совпадении характеристик сетевого пакета с его описанием в правиле выполняется заданное действие. Если доступ запрещен, дальнейшая проверка пакета на соответствие оставшимся правилам не выполняется. Если доступ разрешен, выполняется дальнейшая проверка пакета. Пакеты сетевого трафика, не попавшие под действие ни одного из правил, пропускаются.

Примечание. Служебные правила, пропускающие сетевой трафик, необходимый для работы Secret Net Studio, применяются даже если предыдущие уровни проверок заблокировали пакет.

Порядок обработки пакетов для прикладных правил:

- сначала выполняется обработка пакетов, соответствующая обработке входящего трафика;
- после преобразования данных в операции над общими папками и именованными каналами выполняется проверка на соответствие прикладным правилам;
- после выполнения операций над общими папками и именованными каналами и последующего преобразования ответа в исходящие пакеты выполняется обработка, соответствующая проверке исходящего трафика.

Если операции над общими папками и именованными каналами выполняются непосредственно защищаемым компьютером, проверка на соответствие прикладным правилам не выполняется.

Управление приоритетом правила

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.

Средства Secret Net Studio позволяют изменять приоритет обработки правил.

Для управления приоритетом правила:

1. Выберите в списке правило, приоритет которого требуется изменить.
2. Измените приоритет правила с помощью кнопок "Вниз" и "Вверх".

Управление правилами доступа

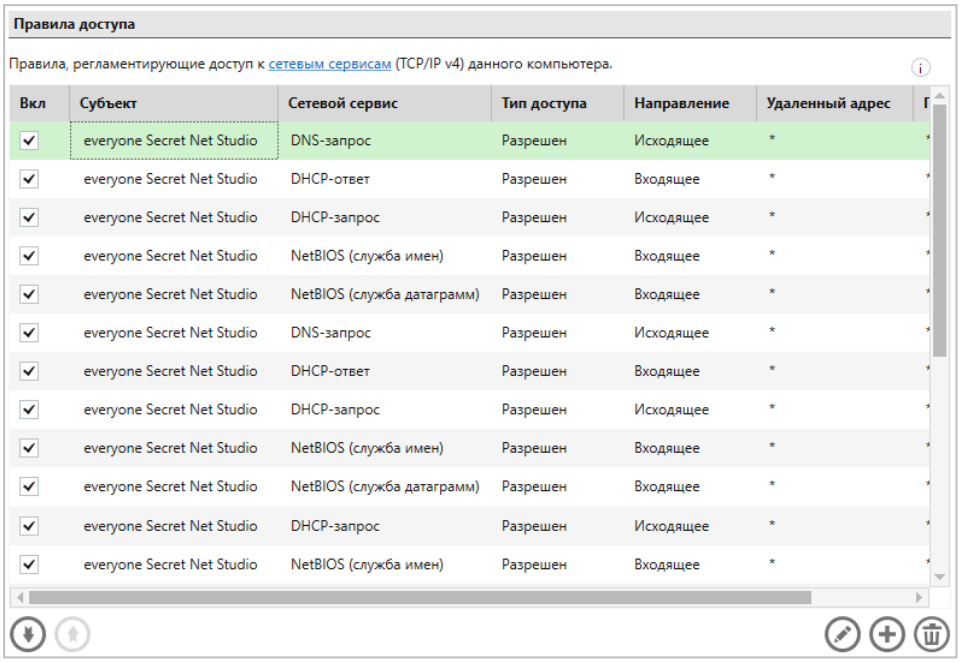
Правила доступа регулируют доступ аутентифицированных и анонимных пользователей к сетевым сервисам защищаемого компьютера. Данные правила имеют более высокий приоритет, чем прикладные правила (см. стр.225).

Внимание!

- По умолчанию правила доступа применяются для всех сетевых интерфейсов компьютера.
- При изменении правил новые настройки вступают в силу в течение 4–6 минут после сохранения изменений.

Для управления правилами:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Правила доступа".



Для каждого правила в таблице отображаются данные:

Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Субъект	Имя учетной записи или группы учетных записей, для которых действует правило
Сетевой сервис	Наименование сетевого сервиса, для которого действует правило
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Направление	Направление трафика, для которого действует правило
Удаленный адрес	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров
Приложение	Путь к приложению, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех приложений

Примечание. При добавлении правил доступа в режиме обучения в таблице будет отображаться столбец с признаком "Автообучение". Чтобы снять признак автообучения, нажмите кнопку "Снять признак самообучения".

2. Выполните нужные действия:
   - создайте правила (см. стр.**214**);
   - измените параметры правил (см. стр.**220**);
   - удалите ненужные правила (см. стр.**221**);
   - определите приоритет правил (см. стр.**212**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Создание правила доступа

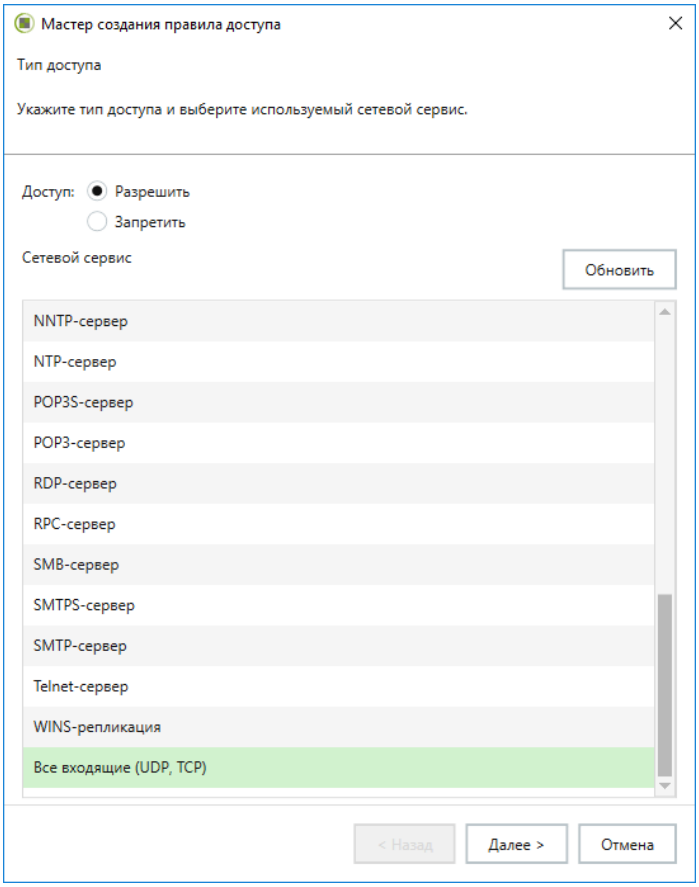
Для создания правила доступа используется специальная программа-мастер.

Совет. Для управления процедурой используйте кнопки:
- "< Назад" — для возврата к предыдущему диалогу;
- "Далее >" — для перехода к следующему диалогу;
- "Отмена" — для прекращения процедуры.

Для создания правила доступа:

1. Нажмите кнопку "Добавить".

   На экране появится первый диалог мастера создания правила.

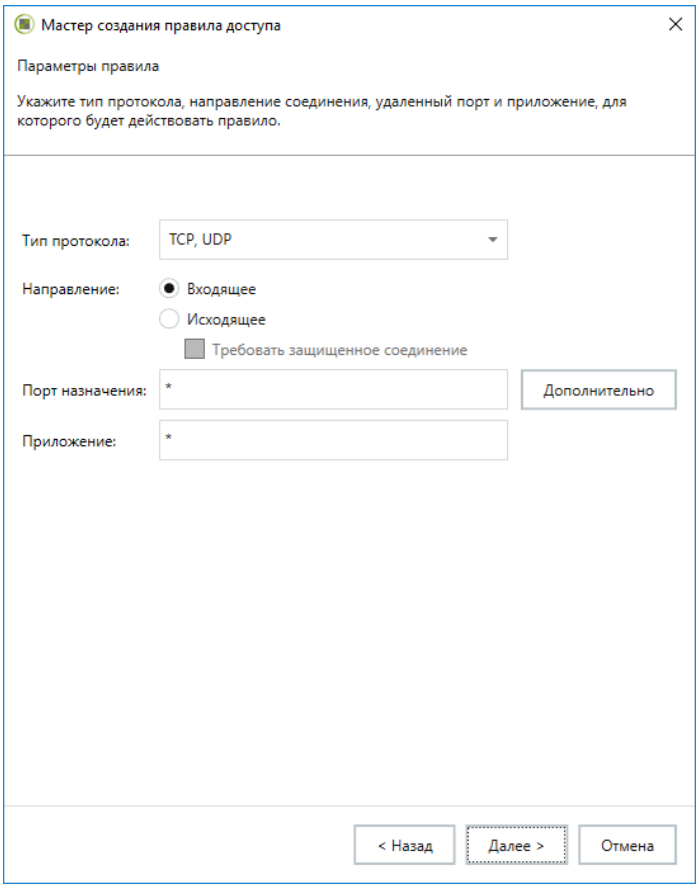


2. Настройте параметры и нажмите кнопку "Далее >".

Поле	Значение
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Сетевой сервис	Выберите в списке название сетевого сервиса для типовой настройки параметров сетевых протоколов в создаваемом правиле. Если эти параметры предполагается настраивать вручную, выберите значение "<пусто>"

Примечание. В списке сетевых сервисов содержатся сервисы, заданные по умолчанию. Чтобы в списке появились сервисы, ранее созданные вручную (см. стр. 239), нажмите кнопку "Обновить".

На экране появится следующий диалог мастера.



Пояснение. Если на предыдущем шаге мастера был выбран сетевой сервис, поля диалога будут настроены в соответствии с его параметрами. В этом случае при изменении данных параметров в полях диалога название выбранного сетевого сервиса будет заменено в правиле кратким описанием заданных параметров. При этом список сетевых сервисов изменен не будет.

3. Заполните поля диалога и нажмите кнопку "Далее >".

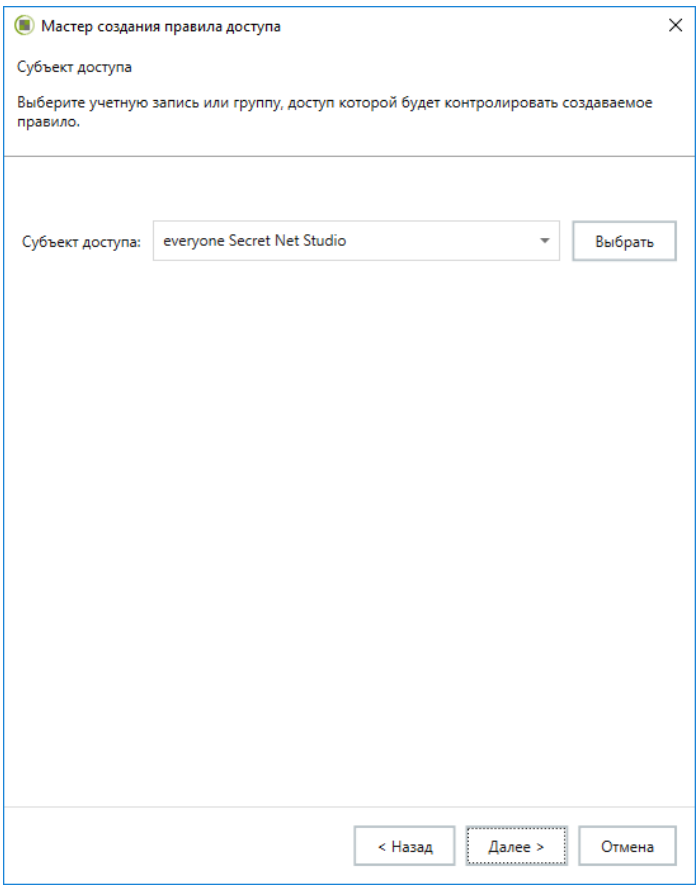
Поле	Значение
Тип протокола	Выберите тип протокола, для которого действует правило
Направление	Укажите направление трафика, для которого действует правило (по отношению к защищаемому объекту)
Требовать защищенное соединение	Отметьте поле, если для исходящего сетевого соединения требуется использовать защищенный канал передачи данных (см. стр.**246**)
Порт назначения	Укажите номера портов, для которых действует правило: • для входящего трафика укажите номера портов, на которые поступают IP-пакеты; • для исходящего трафика укажите номера портов, на которые отправляются IP-пакеты; • оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "-" (дефис). Нажмите кнопку "Дополнительно", если требуется настроить перечень портов в диалоговом режиме

Поле	Значение
Приложение	Укажите путь к исполняемому файлу приложения, для которого действует правило: • укажите путь к приложению. При указании пути к приложению можно также использовать системные переменные Windows; • оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех приложений. Созданное правило будет регулировать сетевой трафик для приложения, работающего непосредственно на защищаемом компьютере

Внимание! Для корректной работы правил доступа рекомендуется указывать полный путь к исполняемому файлу приложения.

Внимание! При использовании параметра "Требовать защищенное соединение" сетевые соединения по незащищенному каналу не устанавливаются (при наличии лицензии на механизм авторизации сетевых соединений).

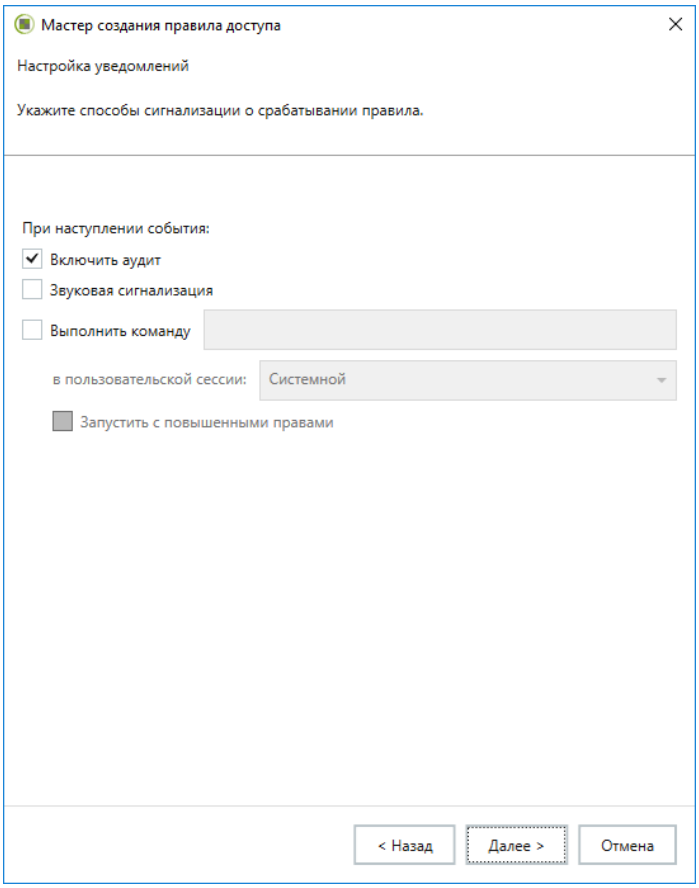
На экране появится диалог для выбора субъекта доступа.



Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать". Данная возможность есть только в сетевом режиме работы Secret Net Studio – C при наличии лицензии на использование механизма авторизации сетевых соединений.

4. Укажите имя учетной записи или группы учетных записей, для которой будет действовать правило, и нажмите кнопку "Далее >".

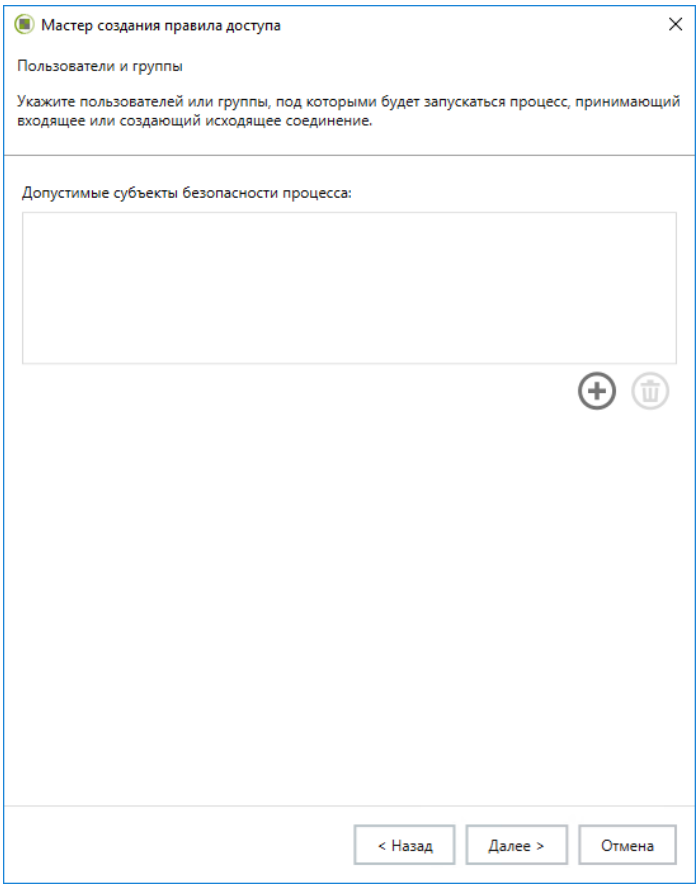
На экране появится диалог настройки уведомлений о срабатывании правила.



5. Укажите способы сигнализации о срабатывании правила, если это необходимо, и нажмите кнопку "Далее >".

Поле	Значение
Включить аудит	Поставьте отметку, если требуется фиксировать в журнале событие, возникающее при срабатывании правила. Если фиксировать событие не требуется — удалите отметку
Звуковая сигнализация	Поставьте отметку, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
Выполнить команду	Поставьте отметку, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. В текстовом поле, которое станет доступным после установки отметки, укажите полный путь и имя исполняемого файла (с параметром). Например, C:\windows\notepad.exe 1.txt
в пользовательской сессии	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: • Системной — выполнить команду с правами системы; • Консольной — выполнить команду от имени пользователя в его сессии; • Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях
Запустить с повышенными правами	Поставьте отметку, чтобы выполнить команду с полными правами пользователя, даже если для пользователя включен контроль учетных записей (UAC, User Account Control)

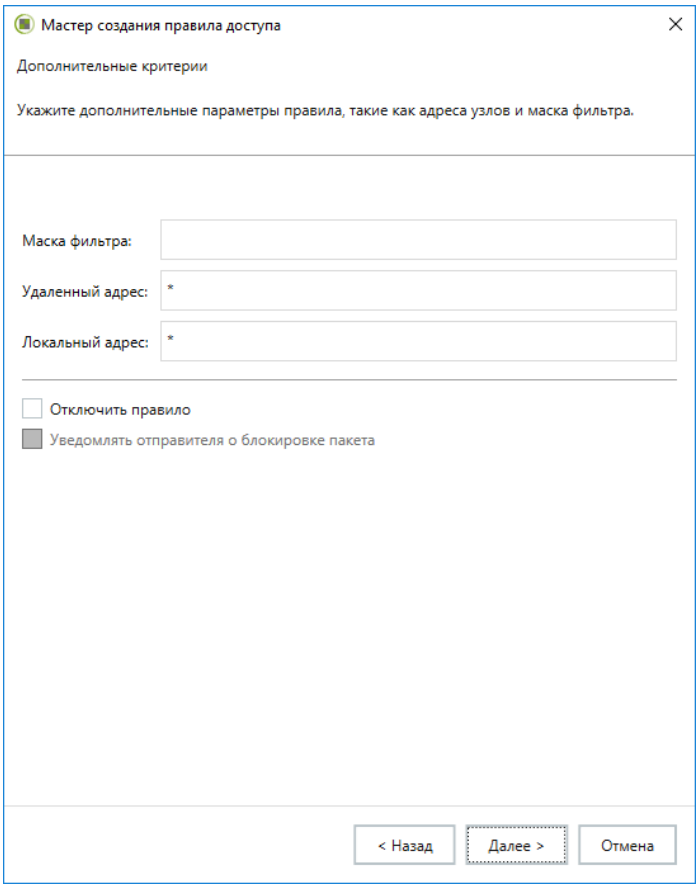
На экране появится диалог для выбора допустимых субъектов безопасности процессов.



Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Добавить". Чтобы удалить учетную запись из списка допустимых, выделите ее и нажмите кнопку "Удалить".

6. Укажите имя учетной записи или группы учетных записей, от имени которой будут запущены процессы, для которых будет действовать правило, и нажмите кнопку "Далее >".

На экране появится диалог для настройки дополнительных параметров.



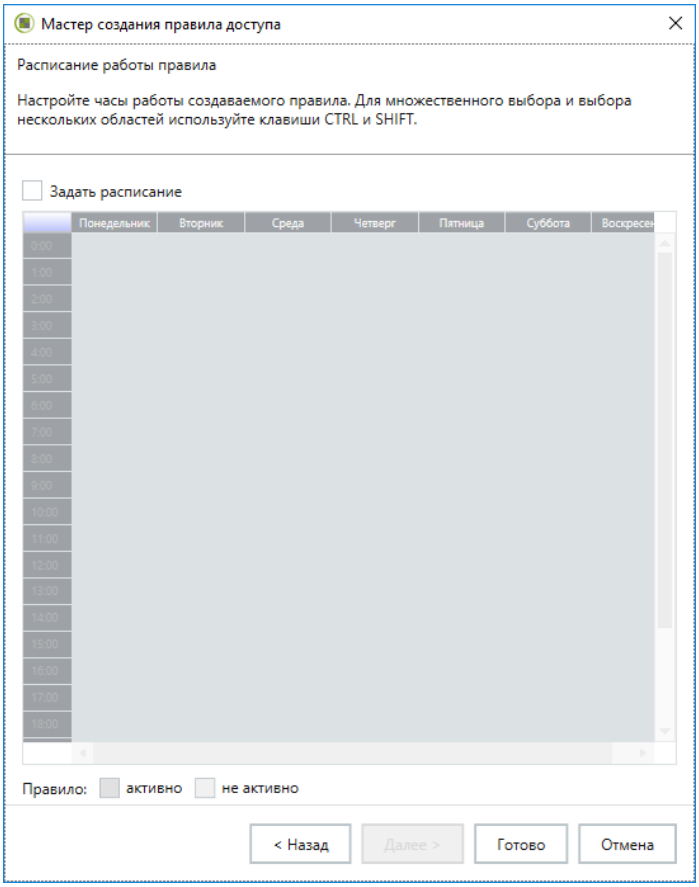
7. Укажите дополнительные параметры правила и нажмите кнопку "Далее >".

Поле	Значение
Маска фильтра	Введите значение, определяющее необходимость обработки IP-пакета. Если поле заполнено, правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Поле поддерживает следующие специальные символы: • * — любое количество символов; • ? — один символ. Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd
Удаленный адрес	Чтобы задать допустимый набор удаленных адресов, укажите имя, IP-адрес компьютера, диапазон IP-адресов (например, 192.168.0.3-192.168.0.9) или подсеть (например, 192.168.1.0/24 или 10.10.0.0/255.255.0.0)
Локальный адрес	Укажите имя, IP-адрес компьютера, диапазон IP-адресов или подсеть, чтобы задать допустимый набор локальных адресов
Отключить правило	Управление работой правила: • отметка отсутствует — правило включено; • отметка установлена — работа правила временно приостановлена
Уведомлять отправителя о блокировке пакета	Управление оповещениями о блокировке пакетов в результате работы запрещающего правила: • отметка отсутствует — отправитель не получает уведомления о блокировке пакетов; • отметка установлена — отправитель получает уведомления о блокировке пакетов. В случае срабатывания правила для протокола TCP будут генерироваться RST-пакеты, для всех остальных протоколов (кроме ICMP, AH, ESP) — пакеты ICMP (тип Destination Unreachable)

Совет. Оставьте в поле "Удаленный адрес" или "Локальный адрес" символ * (звездочка), если требуется, чтобы правило действовало для любых адресов.
Указать несколько IP-адресов, диапазонов адресов или подсетей можно с помощью разделителя ";" (точка с запятой).

Примечание. Поле "Уведомлять отправителя о блокировке пакета" доступно для изменений в правилах с типом доступа "Запретить" и направлением трафика "Входящее".

На экране появится диалог для настройки расписания работы правила.



8. Настройте расписание работы правила, если это необходимо, и нажмите кнопку "Готово":
   - отметьте поле "Задать расписание". Станет доступной для изменения таблица, с помощью которой настраиваются параметры расписания;
   - выделите нажатием левой кнопки мыши ячейки, соответствующие дням недели и времени, в которое требуется разрешить (правило "активно") или запретить (правило "неактивно") работу правила.

Примечание. Время работы правила определяется часовым поясом, установленным для защищаемого компьютера.

Правило будет создано и отобразится в списке правил.

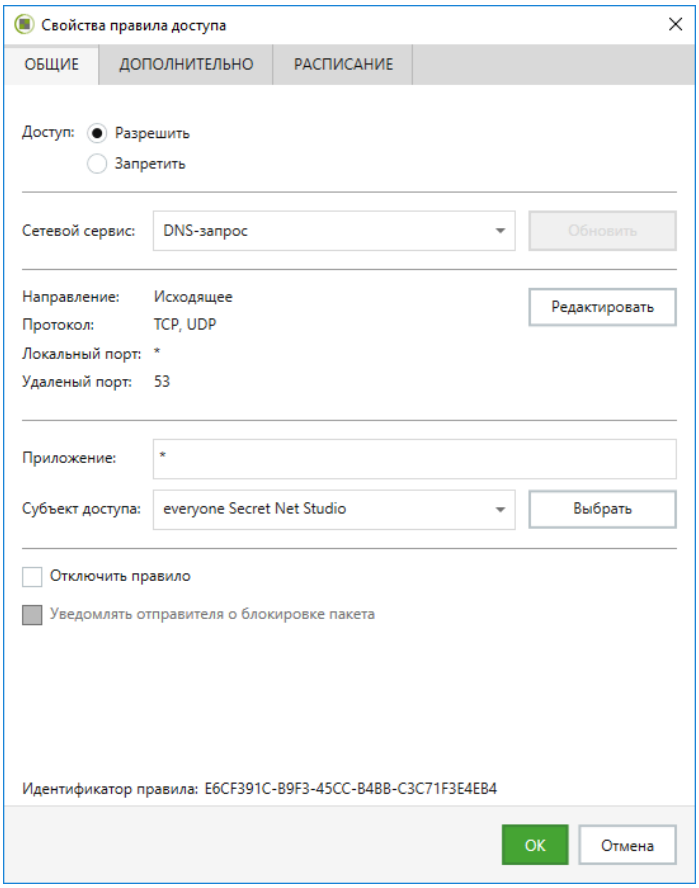
Управление работой правил доступа

Параметры правила доступа, указанные при его создании, могут быть изменены.

Для изменения параметров правила:

1. Выберите в таблице правило доступа, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

На экране появится диалог для настройки параметров правила.



Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.

3. Для управления работой правила:
   - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
   - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "OK".

Внимание! При ошибочном создании правил, осуществляющих блокировку служебных протоколов (DNS, DHCP и т.д.), возможна потеря связи с агентом на удаленном компьютере. В этом случае нужно удалить такие правила в Центре управления (см. ниже), а затем на защищаемом компьютере в командной строке выполнить следующую команду под именем локального администратора:
C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScAuthModCfg.exe /r

Удаление правила доступа

Для удаления правила доступа:

1. Выберите правила, которые требуется удалить.

   Совет. Для выбора нескольких правил используйте клавиши <Ctrl> и <Shift>.

2. Нажмите кнопку "Удалить".

   Выбранные правила будут удалены.

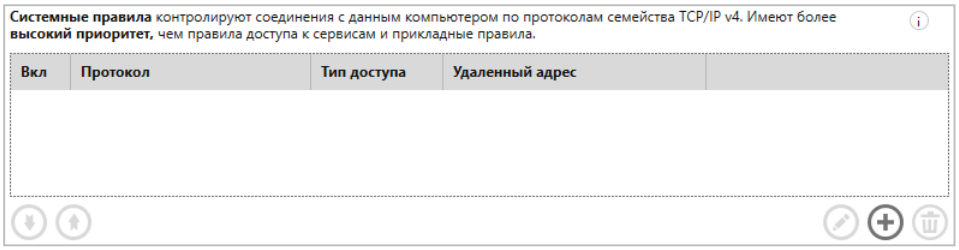
Управление системными правилами

Системные правила контролируют соединения с данным компьютером по протоколам семейства TCP/IP v4. Эти правила имеют более высокий приоритет, чем правила доступа к сетевым сервисам и прикладные правила.

Для управления системными правилами:

1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа".

   На экране появится таблица с перечнем системных правил.



   Для каждого правила отображаются следующие данные.

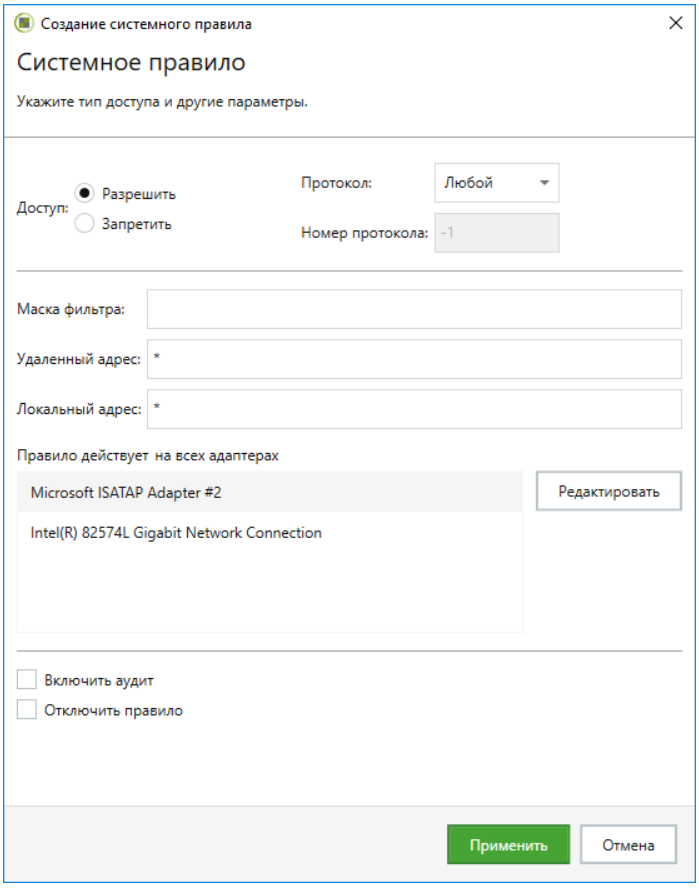
Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Протокол	Наименование протокола, для которого действует правило
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Удаленный адрес	Адрес компьютера, для которого действует правило, или символ * (звездочка), если правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
   - создайте правила (см. стр.**223**);
   - измените параметры правил (см. стр.**224**);
   - удалите ненужные правила (см. стр.**221**);
   - определите приоритет правил (см. стр.**212**);
   - настройте режим защиты протокола ICMP (см. стр.**238**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Создание системного правила

Для создания правила:

1. Нажмите кнопку "Добавить".
   На экране появится диалог для создания системного правила.



2. Настройте параметры правила и нажмите кнопку "Применить".

Поле	Значение
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Протокол	Выберите тип протокола, для которого действует правило, или: • "Любой" — если нужно, чтобы правило действовало для всех указанных в списке типов протоколов; • "Другой"— если нужный тип протокола отсутствует в списке. В этом случае станет доступным для изменения поле "Номер протокола"
Номер протокола	Если выбран тип протокола, то значение в этом поле устанавливается автоматически и изменить его нельзя. Если в поле "Протокол" выбрано значение "Другой", укажите номер протокола, для которого действует правило

Поле	Значение
Маска фильтра	Введите значение, определяющее необходимость обработки IP-пакета. Если поле заполнено, правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Поле поддерживает следующие специальные символы: • * — любое количество символов; • ? — один символ. Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd
Удаленный адрес	Укажите имя, IP-адрес компьютера, диапазон IP-адресов (например, 192.168.0.3-192.168.0.9) или подсеть (например, 192.168.1.0/24 или 10.10.0.0/255.255.0.0), чтобы задать допустимый набор удаленных адресов. Оставьте символ ***** (звездочка), если требуется, чтобы правило действовало для всех удаленных компьютеров
Локальный адрес	Укажите имя, IP-адрес компьютера, диапазон IP-адресов или подсеть, чтобы задать допустимый набор локальных адресов. Оставьте символ ***** (звездочка), если требуется, чтобы правило действовало для всех локальных компьютеров
Правило действует ...	Чтобы правило действовало только на определенных адаптерах, нажмите кнопку "Редактировать" и выберите нужные адаптеры
Включить аудит	Управление регистрацией событий, возникающих при срабатывании данного правила: • отметка отсутствует — регистрация событий выключена; • отметка установлена — регистрация событий включена
Отключить правило	Управление работой правила: • отметка отсутствует — правило включено; • отметка установлена — работа правила временно приостановлена

Новое правило отобразится в списке правил.

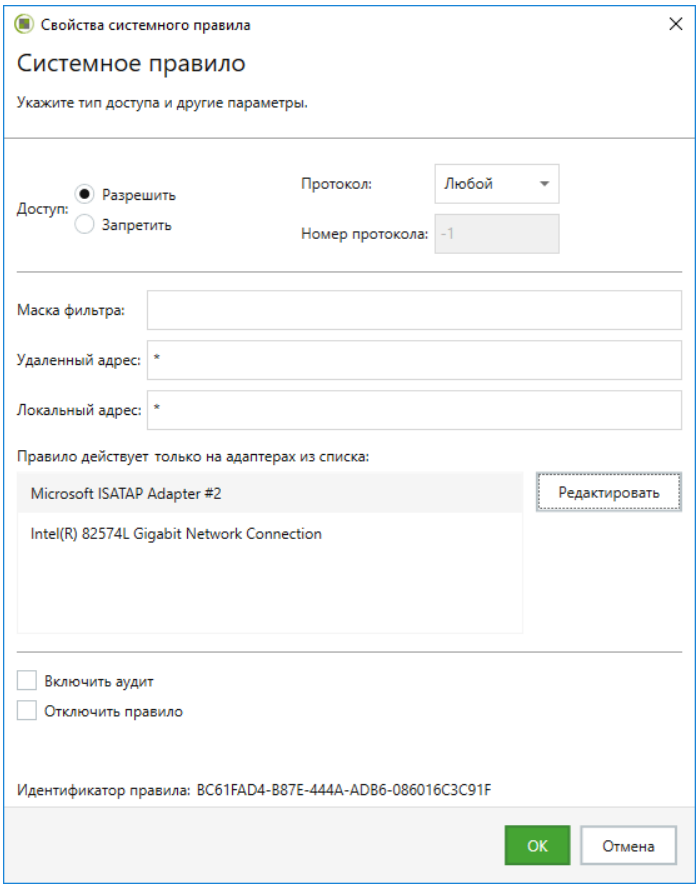
Управление работой системных правил

Параметры системного правила, указанные при его создании, можно изменить.

Для изменения параметров системного правила:

1. Выберите в таблице правило, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

На экране появится диалог для настройки параметров правила.



Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.

3. Для управления работой правила:
   - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
   - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "ОК".

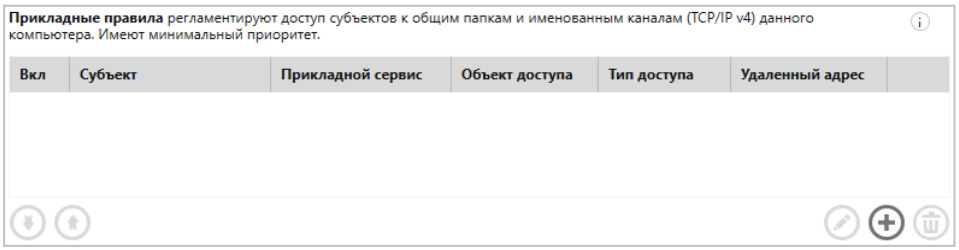
Управление прикладными правилами

Прикладные правила регулируют доступ аутентифицированных и анонимных пользователей к общим папкам и именованным каналам на данном компьютере. Данные правила имеют минимальный приоритет.

Для управления правилами:

1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа".

   На экране появится таблица с перечнем прикладных правил.



Для каждого правила отображаются данные:

Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Субъект	Имя учетной записи или группы учетных записей, для которых действует правило
Прикладной сервис	Наименование прикладного сервиса: • "Общие папки"; • "Именованные каналы"
Объект доступа	Наименование общей папки или именованного канала, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех объектов этого типа
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Удаленный адрес	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
   - создайте правила (см. стр.**226**);
   - измените параметры правил (см. стр.**232**);
   - удалите ненужные правила (см. стр.**221**);
   - определите приоритет правил (см. стр.**212**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

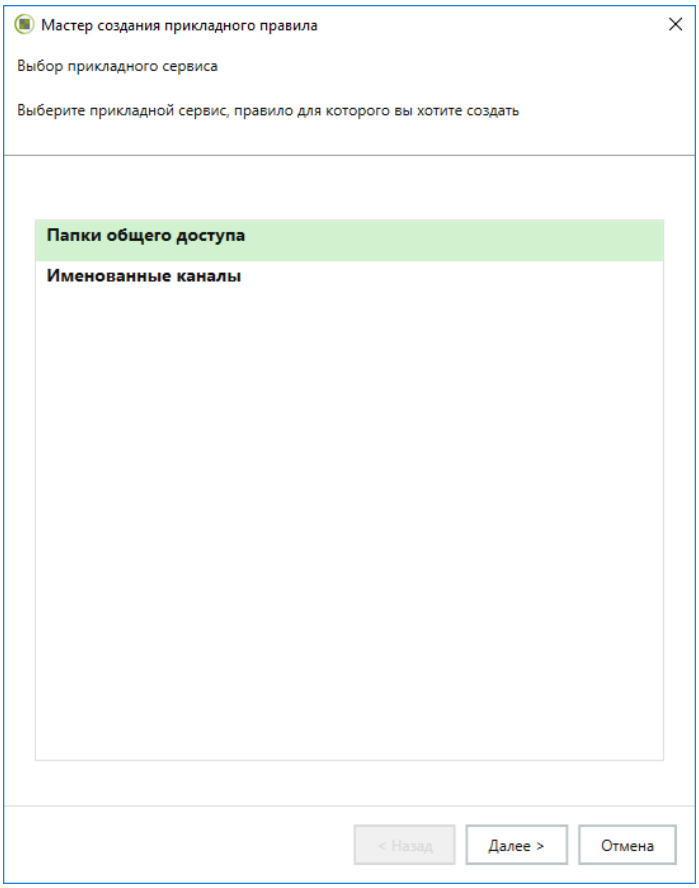
Создание прикладного правила

Для создания прикладного правила используется специальная программа-мастер.

Для создания правила:

1. Нажмите кнопку "Добавить".

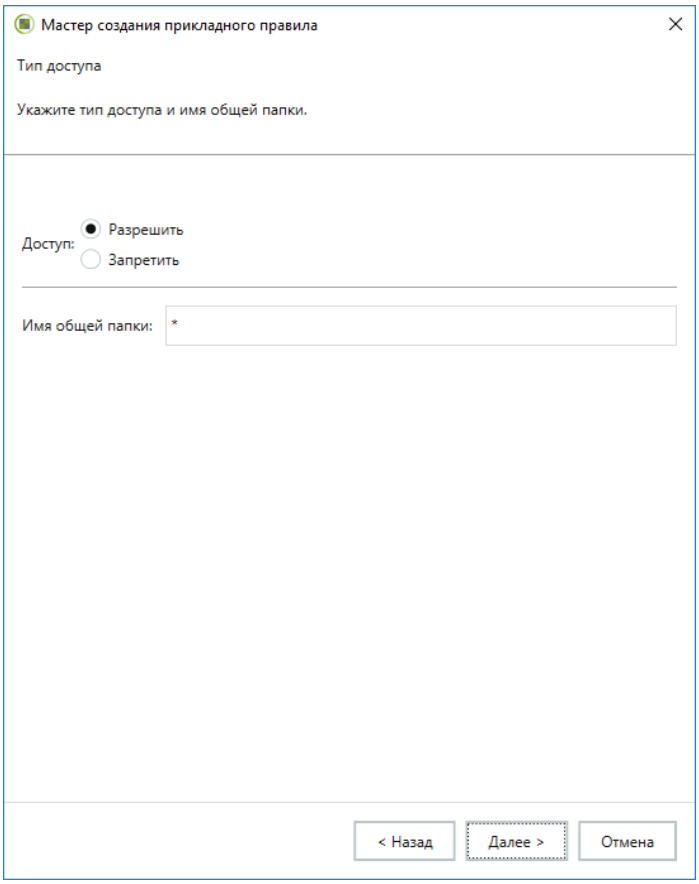
На экране появится первый диалог мастера создания правила.



2. Выберите прикладной сервис, правило для которого вы хотите создать, и нажмите кнопку "Далее >":
   - "Папки общего доступа" — новое правило будет контролировать доступ пользователей к указанной сетевой общей папке по протоколу SMB;
   - "Именованные каналы" — новое правило будет контролировать доступ пользователей к указанному именованному каналу по протоколу Named Pipes.

Примечание. Прикладные правила позволяют разграничить доступ пользователей к общим папкам со всем их содержимым (например, \\server\share). Гранулярное разграничение доступа к подпапкам общих папок (например, \\server\share\folder) не обеспечивается.

На экране появится диалог для настройки параметров правила.



3. Укажите параметры и нажмите кнопку "Далее >".

Поле	Значение
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Имя общей папки/ Именованный канал	Укажите название папки или канала, для которой(ого) действует правило. Оставьте символ * (звездочка), если правило будет действовать для всех папок или именованных каналов на данном компьютере

Пояснение.

- Имя общей папки указывается без имени компьютера, на котором она находится. Например, если сетевой путь к папке на сервере \\server\share, то укажите в поле только ее имя: share.
- В имени папки или канала могут быть использованы подстановочные символы: ? (вопросительный знак) — для замены одного символа и * (звездочка) — для замены нескольких символов, включая пробел.
- Если доступ к общим папкам защищаемого объекта запрещен для всех пользователей (создано запрещающее правило для учетной записи everyone, в котором в качестве имени общей папки указан символ * (звездочка)), то для того чтобы пользователи имели возможность просматривать список общих папок на данном компьютере, необходимо создать разрешающее правило для общей папки IPC$.

На экране появится диалог для выбора учетных записей, для которых действует правило.

4. Укажите имя учетной записи или группы учетных записей, для которой будет действовать правило, и нажмите кнопку "Далее >".

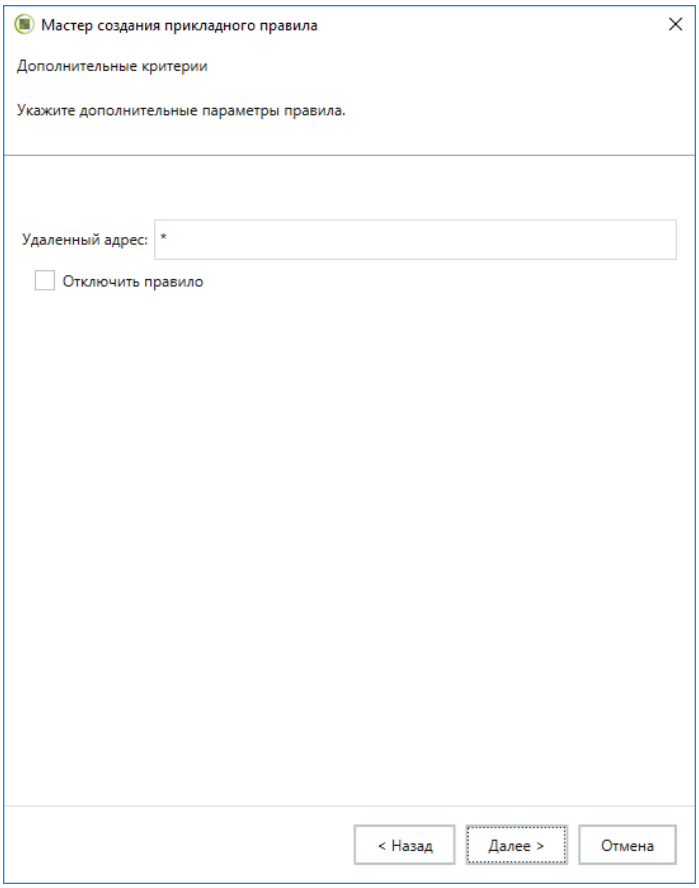
Совет. Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать".

На экране появится диалог для настройки уведомлений о срабатывании правила.

5. Укажите способы сигнализации о срабатывании правила, если это необходимо, и нажмите кнопку "Далее >".

Поле	Значение
Включить аудит	Отметьте, если требуется фиксировать в журнале событие, возникающее при срабатывании этого правила. Если фиксировать событие не требуется — удалите отметку
Звуковая сигнализация	Отметьте, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
Выполнить команду	Отметьте, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. В текстовом поле, которое станет доступным после установки отметки, укажите полный путь и имя исполняемого файла (с параметром). Например, C:\windows\notepad.exe 1.txt
в пользовательской сессии	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: • Системной — выполнить команду с правами системы; • Консольной — выполнить команду от имени пользователя в его сессии; • Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях
Запустить с повышенными правами	Поставьте отметку, чтобы выполнить команду с полными правами пользователя, даже если для пользователя включен контроль учетных записей (UAC, User Account Control)

На экране появится диалог для настройки дополнительных параметров.



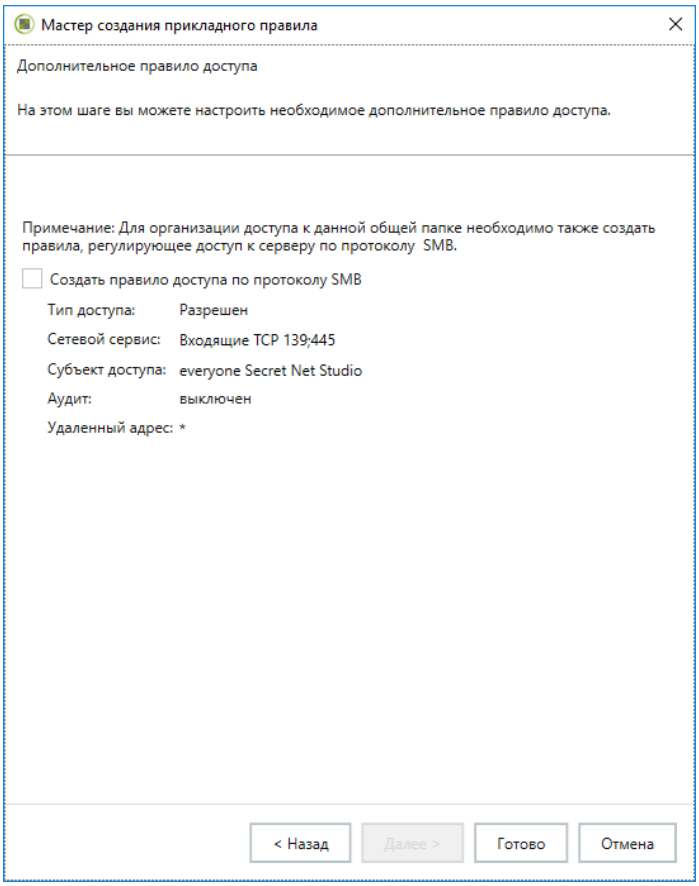
6. Укажите дополнительные параметры правила и нажмите кнопку "Далее >".

Поле	Значение
Удаленный адрес	Укажите имя или IP-адрес компьютера (маску подсети), к которому будет применяться правило при попытке доступа к общей папке или именованному каналу на защищаемом компьютере. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех компьютеров, осуществляющих попытку доступа
Отключить правило	Отметьте поле, если требуется ввести правило в эксплуатацию позднее

На экране появится диалог для настройки расписания работы правила.

7. Настройте расписание работы правила, если это необходимо, и нажмите кнопку "Далее >":
   - отметьте поле "Задать расписание". Станет доступной для изменения таблица, с помощью которой настраиваются параметры расписания;
   - выделите нажатием левой кнопки мыши ячейки, соответствующие дням недели и времени, в которое требуется разрешить (правило "активно") или запретить (правило "неактивно") работу правила.

На экране появится диалог создания дополнительного правила доступа.



Для корректной работы прикладных правил необходимо также настроить правила прохождения IP-пакетов на транспортном уровне — по протоколу SMB. Для этого требуется создать правило доступа, разрешающее прохождение пакетов по протоколу TCP на порт 445 (и/или 139) для учетной записи (группы), указанной в прикладном правиле.

Внимание! Если прохождение пакетов по протоколу SMB запрещается, прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.

8. Если требуется создать разрешающее правило доступа по протоколу SMB — отметьте поле "Создать правило доступа по протоколу SMB".
9. Нажмите кнопку "Готово".

   Новое правило будет добавлено в список прикладных правил.

   При использовании функции создания дополнительного SMB-правила в списке правил доступа также отобразится правило, разрешающее использование SMB для учетной записи (группы), указанной в прикладном правиле.

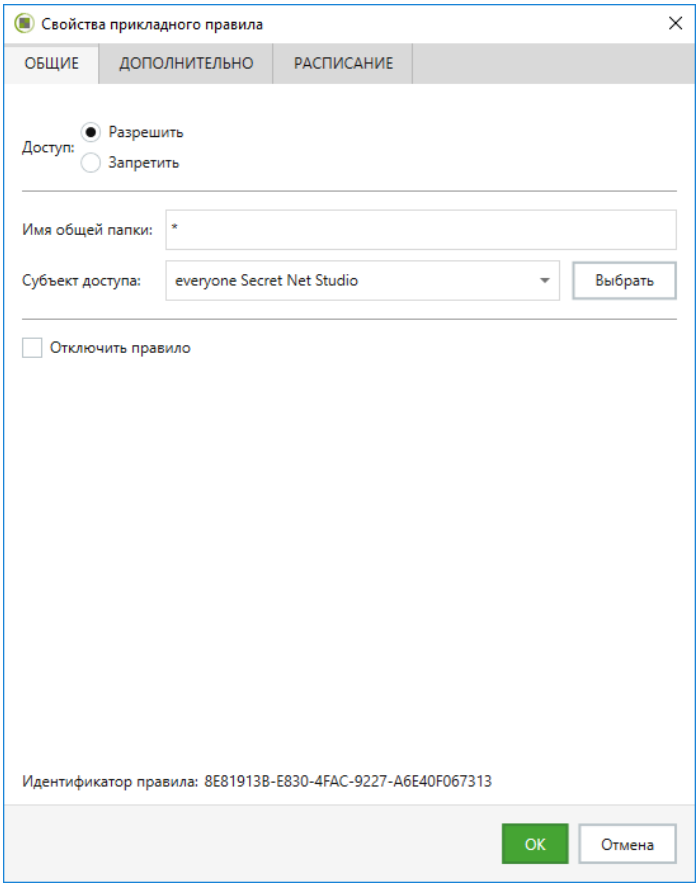
Управление работой прикладных правил

Параметры прикладного правила, указанные при его создании, могут быть изменены.

Для изменения параметров правила:

1. Выберите в таблице прикладное правило, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

   На экране появится диалог для настройки параметров правила.



   Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.
3. Для управления работой правила:
   - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
   - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "ОК".

Управление правилами фильтрации сетевого потока

Правила фильтрации сетевого потока предназначены для осуществления фильтрации команд сетевых протоколов, параметров команд, а также для управления доступом к ресурсам, содержащим отдельные типы мобильного кода.

Управление правилами фильтрации сетевого потока осуществляется с помощью утилиты командной строки ScAuthSrvConfig.exe (в сетевом режиме работы Secret Net Studio) или ScLocalSrvConfig.exe (в автономном режиме работы).

Утилита ScAuthSrvConfig.exe располагается на сервере безопасности в папке установки, по умолчанию — Secret Net Studio\Server\Authentication Server\.

Примечание. Для входа в режим управления конфигурацией утилите ScAuthSrvConfig.exe нужно передать параметры для подключения к серверу управления (см. ниже).

Утилита ScLocalSrvConfig.exe располагается на защищаемом компьютере в папке установки, по умолчанию — Secret Net Studio\Client\Components \Network Protection\.

Внимание! Для изменения локальной конфигурации с помощью утилиты ScLocalSrvConfig.exe требуется наличие прав локального администратора.

Подключение к серверу управления

Для входа в режим управления конфигурацией утилите ScAuthSrvConfig.exe нужно передать параметры для подключения к серверу управления. Для этого откройте командную строку и выполните следующую команду:

```
ScAuthSrvConfig.exe [@argfile] [/?|h|help] [/v|version]
<domain> [/local] [kdc] [/p|password <value>] [/a|admin
<value>] [/q <value>] [/s <value>]
```

где:

- @argfile — прочитать аргументы из файла;
- /? — показать подробную информацию об утилите;
- /v — показать номер версии утилиты;
- domain — домен Kerberos;
- /local — локальный режим (восстановление конфигурации);
- kdc — расположение KDC (Key Distribution Center);
- /p <value> — пароль администратора домена;
- /a <value> — имя администратора домена;
- /q <value> — команда выполнения запроса;
- /s <value> — путь к script-файлу для исполнения.

Пример

Подключение к серверу управления, запущенному на данном компьютере:

```
ScAuthSrvConfig.exe DOMAINNAME 127.0.0.1 /admin Administrator
```

где:

- DOMAINNAME — домен безопасности;
- 127.0.0.1 — сетевой адрес сервера конфигурации;
- Administrator — имя администратора Secret Net Studio.

Создание и редактирование правил фильтрации сетевого потока

Для добавления нового правила фильтрации сетевого потока введите следующую команду в командной строке утилиты:

```
add network_stream_filtration_rule <protected_computer>
/filter <value> [/flt-case-insensetive | /flt-case-sensetive]
[/at allow|deny] [/order <value>] [/local_addrs <value>]
[/local_ports <value>] [/remote_addrs <value>] [/remote_ports
<value>] [/direction <value>] [/audit 1|0] [/enable 1|0]
```

Доступны следующие команды и параметры правила:

Параметр	Описание	Возможные значения
add network_ stream_filtration_ rule или add nsfr	Команда для создания правила фильтрации	
modify network_ stream_filtration_ rule или modify nsfr	Команда для редактирования правила фильтрации	
protected_ computer	Полное доменное имя защищаемого компьютера, для которого будет действовать правило	
filter	Маска фильтра	• * — заменяет любое количество символов; • ? — заменяет один символ
flt-case-insensetive	Регистронезависимый поиск	
flt-case-sensetive	Регистрозависимый поиск. Применяется по умолчанию	
at (access type)	Тип правила доступа	• deny — при обнаружении последовательности, попадающей под маску фильтра, соединение будет разорвано. Значение задано по умолчанию; • allow — при обнаружении последовательности, попадающей под маску фильтра, будет выполнен только аудит (если он разрешен)
direction	Список направлений соединений (сетевого трафика), для которых будет применяться это правило. В качестве разделителя используется ";"	• in — правило будет применяться для входящих соединений, для входящего трафика. Значение задано по умолчанию; • in_reply — правило будет применяться для входящих соединений, для ответного трафика; • out — правило будет применяться для исходящих соединений, для исходящего трафика; • out_reply — правило будет применяться для исходящих соединений, для ответного трафика
local_addrs	Список локальных адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
local_ports	Список локальных портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	

Параметр	Описание	Возможные значения
remote_addrs	Список удаленных адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
remote_ports	Список удаленных портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
audit	Включение/выключение аудита при срабатывании правила	• 1 — аудит включен; • 0 — аудит выключен
order	Порядок применения правил. Параметр влияет только на порядок срабатывания правил	
enable	Текущий статус правила	• 1 — правило включено; • 0 — правило выключено

Для редактирования правила фильтрации используется следующая команда:

```
modify network_stream_filtration_rule(nsfr) <protected_
computer> <rule_id> [/filter <value>] [/at allow|deny]
[/order <value>] [/local_addrs <value>] [/local_ports
<value>] [/remote_addrs <value>] [/remote_ports <value>]
[/direction <value>] [/audit 1|0] [/enable 1|0]
```

где <rule_id> — идентификатор правила, которое нужно модифицировать.

Примеры

Пример 1. Фильтрация одиночной команды

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемой команде "cmd".

```
add nsfr SP-VM01 /filter "cmd1" /direction out /remote_ports
23
```

Пример 2. Фильтрация последовательности команд

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемых данных последовательности команд "cmd1", "cmd2" и "cmd3", между которыми может быть любое количество символов.

```
add nsfr SP-VM01 /filter "cmd1*cmd2*cmd3" /direction out
/remote_ports 23
```

Пример 3. Фильтрация параметра команды

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемых данных команды "cmd" с параметром "param".

```
add nsfr SP-VM01 /filter "cmd*param" /direction out /remote_
ports 23
```

Пример 4. Фильтрация доступа к ресурсам, содержащим отдельные типы мобильного кода

Для фильтрации доступа к ресурсам, содержащим отдельные типы мобильного кода, применяются правила фильтрации сетевого потока, в которых в качестве фильтра используются текстовые последовательности, характерные для мобильного кода определенного типа. Например, в протоколе HTTP для запрета мобильного кода необходимо создавать правила для исходящих соединений, для ответного трафика, с фильтрацией по заголовку "Content-Type". Дополнительно фильтрация может быть выполнена с помощью проверки заголовка "Content-Disposition" и его параметра "filename".

Список заголовков "Content-Type" для разных типов мобильного кода:

Тип мобильного кода	Строка для фильтрации
JavaScript	Content-Type: text/javascript Content-Type: text/jscript Content-Type: text/x-javascript Content-Type: text/ecmascript Content-Type: text/x-ecmascript Content-Type: application/javascript Content-Type: application/x-javascript Content-Type: application/ecmascript Content-Type: application/x-ecmascript
Adobe Flash	Content-Type: application/x-shockwave-flash
VBScript	Content-Type: text/vbscript
Java	Content-Type: application/java-archive Content-Type: application/jar
ActiveX	Content-Type: application/ocx Content-Type: application/x-ms

Пример создания набора правил для фильтрации мобильного кода:

```
add nsfr SP-VM01 /filter "Content-Type: application/ocx"
/flt-case-insensetive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter "Content-Type: application/x-ms"
/flt-case-insensetive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter " Content-Disposition*filename*ocx"
/flt-case-insensetive /direction out_reply /remote_ports 80
```

Правила блокируют загрузку ActiveX- компонентов по протоколу HTTP, работающему через 80 порт.

Просмотр правил фильтрации сетевого потока

Чтобы просмотреть список правил фильтрации сетевого потока, выполните команду:

```
show network_stream_filtration_rules(nsfrs) <protected_
computer>
```

где <protected_computer> — имя защищаемого компьютера.

Пример

```
show nsfrs SP-VM01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
direction out
proto 6
local-addr *(*)
remote-addr *(23)
```

Просмотреть детальную информацию об отдельном правиле фильтрации сетевого потока можно с помощью команды:

```
show network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

где:

- <protected_computer> — имя защищаемого компьютера;
- <id> — идентификатор правила.

Пример

```
show nsfr SP-VM01 {ca541ade-b955-4cf2-8894-d020aac9d9ac}
server: sp-vm01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
enabled 1
direction out
proto 6
local-addr *(*)
remote-addr *(23)
audit 1
```

Удаление правила фильтрации сетевого потока

Чтобы удалить правило фильтрации сетевого потока, выполните команду:

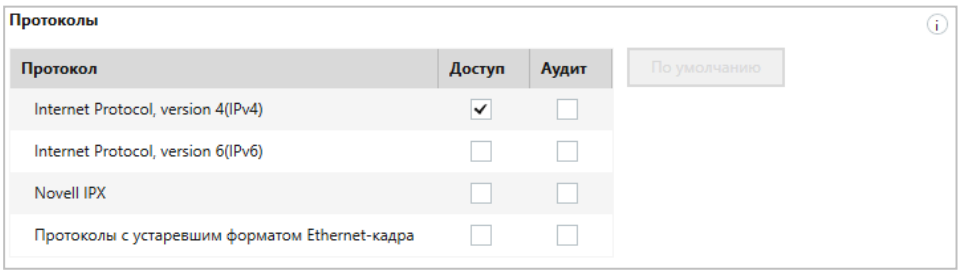
```
delete network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

Управление сетевыми протоколами

Средства Secret Net Studio позволяют настроить доступ к защищаемым компьютерам по протоколам сетевого уровня IPv4, IPv6, Novell IPX, а также некоторым протоколам с устаревшим форматом Ethernet-кадра (LLC, IPX). По умолчанию работа этих протоколов запрещается, за исключением протокола IPv4. Эти настройки имеют более высокий приоритет, чем правила доступа к сетевым сервисам, прикладные правила и системные правила.

Для управления сетевыми протоколами:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Настройки | Протоколы".



2. В столбце "Доступ" удалите отметки из ячеек протоколов, которые требуется отключить. Для включения протоколов поставьте отметки.

   Внимание! По умолчанию доступ к защищаемым компьютерам разрешен только по протоколу IPv4. Не рекомендуется разрешать доступ по остальным протоколам, так как сетевой трафик по ним не контролируется межсетевым экраном Secret Net Studio.

3. В столбце "Аудит" отметьте ячейки тех протоколов, для которых требуется фиксировать в журнале события прохождения каждого пакета. Если фиксировать события не требуется — удалите отметку.

   По умолчанию режим аудита для всех протоколов выключен.

Внимание! При включенном режиме аудита количество регистрируемых в журнале Secret Net Studio событий будет очень большим. Это может замедлить работу системы.

Пояснение. Значение поля "Аудит" в настройках сетевых протоколов не связано со значением поля "Включить аудит" в свойствах правил доступа.

4. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

Совет. Для возврата таблицы к первоначальному состоянию используйте кнопку "По умолчанию".

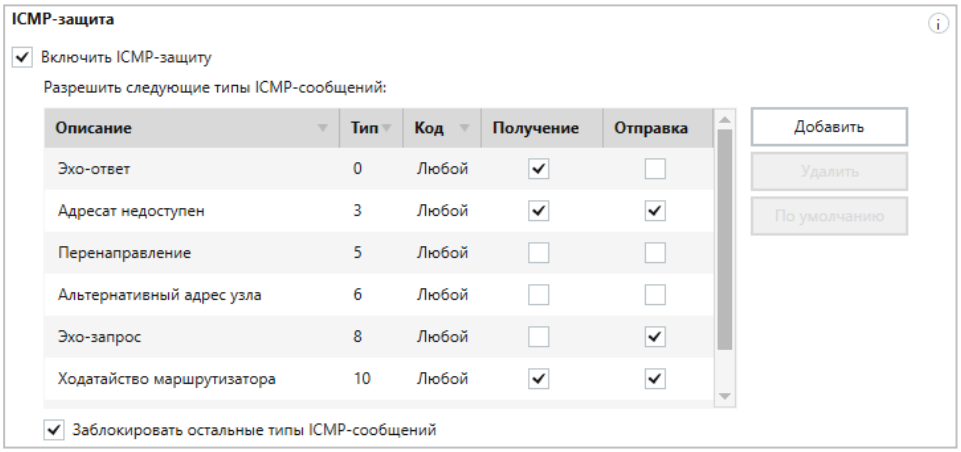
Настройка "Протоколы с устаревшим форматом Ethernet-кадра" позволяет заблокировать Ethernet-кадры, в заголовке которых вместо типа кадра содержится значение его длины. Посредством таких кадров на защищаемый сервер может пройти трафик IPX, SMB поверх NetBEUI и даже IP-трафик.

Настройка режима защиты протокола ICMP

Режим защиты протокола ICMP используется для организации обмена сообщениями по данному протоколу. По умолчанию режим управления пакетами протокола ICMP выключен.

Для настройки параметров режима:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Настройки | ICMP-защита".



Типы пакетов протокола ICMP представлены в виде таблицы. Для каждого типа отображаются следующие данные:

- описание типа пакета;
- тип пакета;
- код пакета;
- средства управления прохождением пакетов.

2. Настройте нужные параметры.

Параметр	Значение
Включить ICMP-защиту	Отметьте поле, если требуется включить защиту ICMP
Столбцы "Получение" и "Отправка"	Разрешите или запретите прохождение входящих и исходящих пакетов. Чтобы разрешить — поставьте отметку в нужную ячейку, чтобы запретить — удалите ее
Заблокировать остальные типы ICMP-сообщений	Отметьте поле, чтобы запретить прохождение всех типов пакетов протокола ICMP, за исключением типов, указанных в таблице. Если требуется снять запрет на прохождение пакетов — удалите отметку

Совет. Используйте кнопки справа от таблицы для добавления типов ICMP-сообщений ("Добавить"), удаления выбранных строк ("Удалить" – нельзя удалить строки, содержащиеся в таблице по умолчанию) или возврата таблицы к первоначальному состоянию ("По умолчанию").

3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

   Режим обработки пакетов протокола ICMP будет настроен в соответствии с указанными параметрами.

Управление сетевыми сервисами

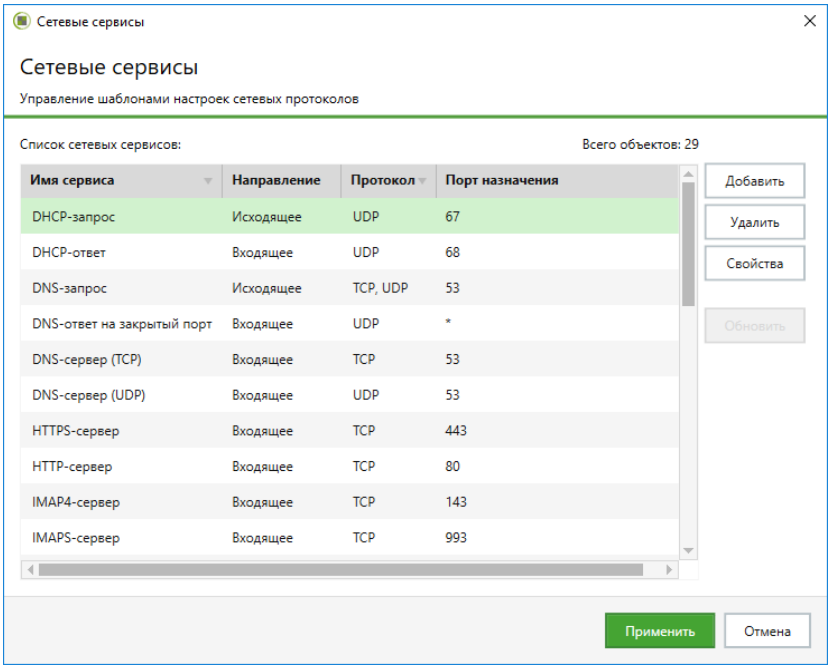
Сетевые сервисы — это список шаблонов наиболее распространенных настроек сетевых протоколов. Для каждого сервиса указываются следующие данные:

- название сетевого сервиса;
- направление трафика, для которого действует сетевой сервис;
- тип протокола сетевого сервиса;
- порт компьютера, для которого действует сетевой сервис.

Для управления сетевыми сервисами:

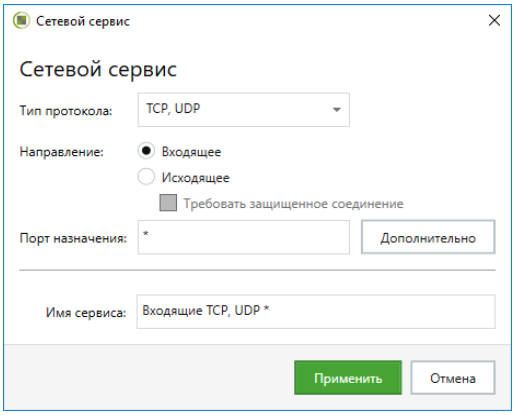
1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "сетевым сервисам".

   На экране появится следующий диалог.



2. Для создания сетевого сервиса нажмите кнопку "Добавить".

   На экране появится диалог для настройки параметров сервиса.



3. Укажите параметры сервиса и нажмите кнопку "Применить".

Параметр	Значение
Тип протокола	Выберите тип протокола для этого сетевого сервиса
Направление	Укажите направление трафика для этого сетевого сервиса: • "Входящее"; • "Исходящее"
Требовать защищенное соединение	Отметьте это поле, если для этого сетевого сервиса требуется использовать защищенное соединение (см. стр.**246**)
Порт назначения	Укажите номера портов для этого сетевого сервиса: • для входящего трафика укажите номера портов, на которые поступают IP-пакеты; • для исходящего трафика укажите номера портов, на которые отправляются IP-пакеты; • оставьте символ * (звездочка), если требуется, чтобы сетевой сервис действовал для всех портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "-" (дефис). Нажмите кнопку "Дополнительно", если требуется настроить перечень портов в диалоговом режиме
Имя сервиса	Введите название, под которым требуется сохранить шаблон сетевого сервиса

Сетевой сервис будет создан и отобразится в списке сетевых сервисов.

4. Для удаления сетевого сервиса выберите его в списке и нажмите кнопку "Удалить".
5. Для изменения параметров сетевого сервиса выберите его в списке и нажмите кнопку "Свойства". В появившемся диалоге измените параметры сервиса, руководствуясь описанием, приведенным в п.**3** данной процедуры, и нажмите кнопку "Применить".
6. Для сохранения изменений нажмите кнопку "Применить" в диалоге настройки сетевых сервисов.
7. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

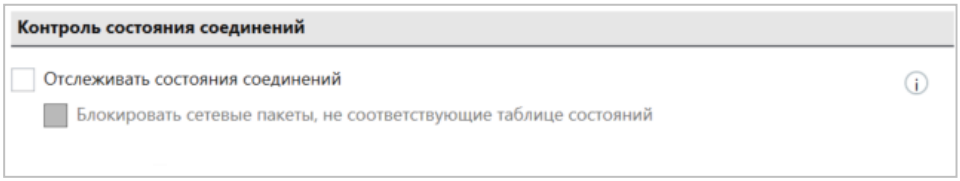
Контроль состояния соединений

Контроль состояния соединений (SPI, Stateful Packet Inspection) позволяет дополнительно защитить компьютеры от сетевых атак, выполняя проверку проходящего трафика. Параметры позволяют вести таблицу состояний устанавливаемых соединений, проверять передаваемый трафик на соответствие таблице и блокировать пакеты, не соответствующие текущему состоянию соединения.

По умолчанию отслеживание состояния соединений отключено.

Для включения контроля состояния соединений:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Контроль состояния соединений".



2. Если требуется включить контроль состояния соединений, отметьте поле "Отслеживать состояние соединений".

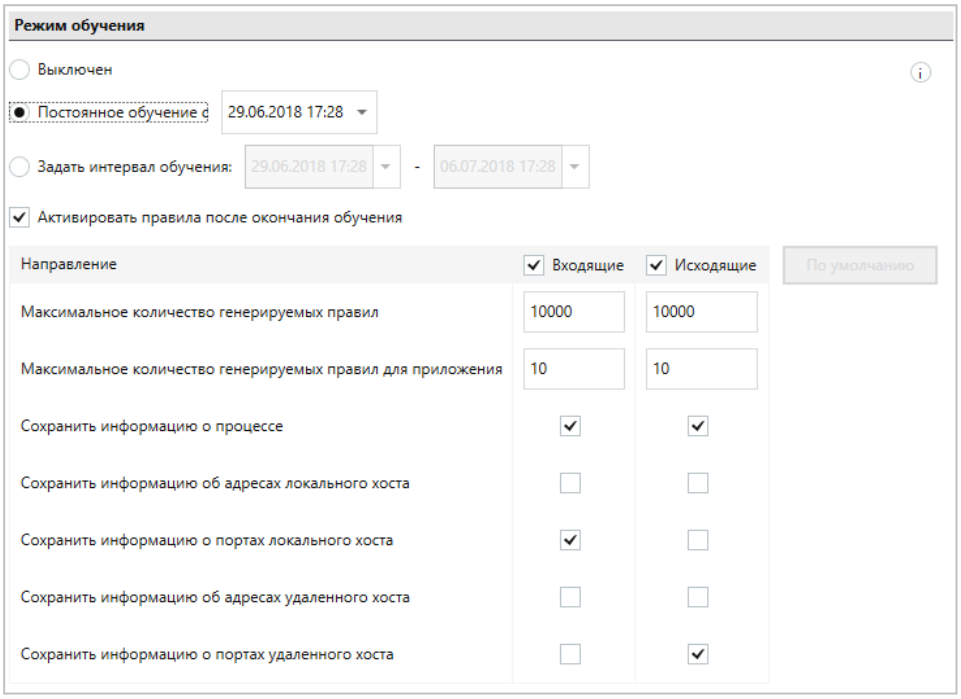
3. При необходимости отметьте поле "Блокировать сетевые пакеты, не соответствующие таблице состояний".

Настройка режима обучения

Режим обучения используется на этапе ввода системы защиты в эксплуатацию. Данный режим позволяет составить базовый набор правил доступа, необходимый для функционирования защищаемого компьютера. Правила доступа составляются на основе информации о сетевой активности приложений на данном компьютере.

Для настройки параметров режима:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Режим обучения".



2. Если требуется включить режим обучения, отметьте поле "Постоянное обучение с" или "Задать интервал обучения" и укажите дату начала обучения или временной интервал.
3. Настройте параметры режима обучения.

Поле	Значение
Активировать правила после окончания обучения	Отметьте поле, чтобы по окончании периода обучения все составленные в его ходе правила доступа начали применяться
Направление	Отметьте направление трафика, для которого будет действовать режим обучения
Максимальное количество генерируемых правил	Укажите максимальное количество правил, генерируемых во время работы режима обучения
Максимальное количество генерируемых правил для приложения	Укажите максимальное количество правил, генерируемых во время работы режима обучения для каждого приложения
Сохранить информацию о процессе	Отметьте поле, чтобы созданные правила действовали для конкретных приложений, процессы которых вызывали сетевую активность. Если поле не отмечено, правила будут созданы для всех приложений

Поле	Значение
Сохранить информацию об адресах/о портах локального/удаленного хоста	Отметьте соответствующие поля для сохранения в составляемых правилах необходимой информации

Совет. Для возврата таблицы к первоначальному состоянию используйте кнопку "По умолчанию".

4. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

   Режим обучения будет настроен в соответствии с указанными параметрами.

Управление работой межсетевого экрана на защищаемых компьютерах

Центр управления Secret Net Studio позволяет осуществлять для отдельного компьютера управление режимом обучения.

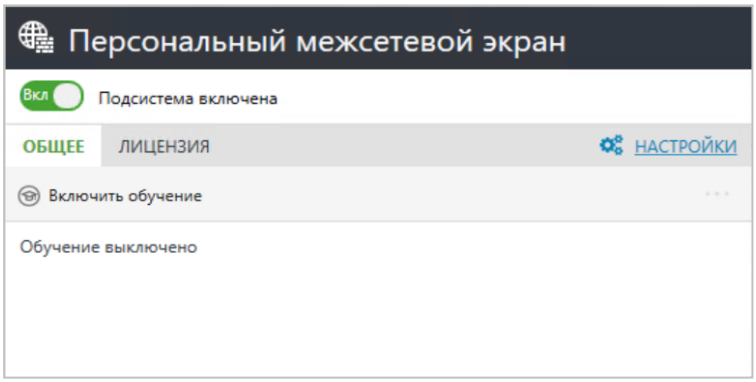
Для управления работой межсетевого экрана:

1. В списке объектов управления выберите нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

   На экране появится информация о состоянии данного компьютера.

2. На вкладке "Состояние" выберите объект "Персональный межсетевой экран".

   В правой части экрана появится панель управления межсетевым экраном.



3. Для включения или отключения межсетевого экрана переведите в нужное положение переключатель в левом верхнем углу панели.
4. Для управления работой режима обучения нажмите кнопку:
   - "Включить обучение" — для включения режима обучения. После этого в панели появятся две следующие кнопки;
   - "Прервать обучение и сохранить правила" — для отключения режима обучения и сохранения всех уже сформированных правил;
   - "Прервать обучение без сохранения правил" — для отключения режима обучения и удаления всех сформированных в ходе обучения правил.

   Режим обучения позволяет сформировать базовый набор правил доступа (см. стр.**241**).

Примечание. Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик межсетевого экрана (см. стр.**211**).

Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Экспорт и импорт конфигурации межсетевого экрана

Экспорт и импорт конфигурации межсетевого экрана Secret Net Studio – C можно выполнить с помощью утилиты командной строки ScAuthSrvConfig (в сетевом режиме работы Secret Net Studio – C) и ScLocalSrvConfig (в автономном режиме).

Примечание. Для входа в режим управления конфигурацией утилите ScAuthSrvConfig.exe нужно передать параметры для подключения к серверу управления (см.стр.232).

Конфигурация межсетевого экрана сохраняется в файле формата XML и может быть использована для восстановления настроек защищаемого компьютера.

Файл конфигурации содержит информацию обо всех настройках и правилах межсетевого экрана.

Экспорт конфигурации

Для экспорта настроек межсетевого экрана откройте командную строку и выполните следующую команду:

```
export account pc_configuration <pc_name> <file_path>
[/append|a]
```

где:

- pc_name — имя защищаемого компьютера;
- file_path — путь к XML-файлу, в который нужно сохранить конфигурацию;
- /append|a — если указан данный флаг, то текущая конфигурация будет добавлена к той, экспорт которой был выполнен ранее в XML-файл.

Импорт конфигурации

Для импорта настроек межсетевого экрана откройте командную строку и выполните следующую команду:

```
import account pc_configuration <pc_name> <file_path>
[/replace]
```

По умолчанию настройки из XML-файла добавляются в текущую конфигурацию защищаемого компьютера, но если указан флаг /replace, то конфигурация защищаемого компьютера будет заменена.

Глава 16
Авторизация сетевых соединений

В Secret Net Studio реализован механизм защиты сетевого взаимодействия между авторизованными абонентами. Данный механизм базируется на открытых стандартах протоколов семейства IPsec и обеспечивает безопасность обмена данными.

Механизм авторизации абонентов основан на протоколе Kerberos. Данный протокол нечувствителен к попыткам перехвата паролей и атакам типа "Man in the Middle". С помощью этого механизма удостоверяются не только субъекты доступа, но и защищаемые объекты. Это предотвращает несанкционированную подмену (имитацию) защищаемой информационной системы с целью осуществления некоторых видов атак.

Механизм авторизации сетевых соединений выполняет следующие функции.

Функция	Описание
Авторизация сетевых соединений	Добавляет специальную служебную информацию для сетевых пакетов, удовлетворяющих правилам, полученным с сервера управления и авторизации. Осуществляет анализ специальной служебной информации входящих пакетов и передачу информации в модуль межсетевого экранирования для осуществления фильтрации по правилам
Контроль неизменности передаваемых сетевых пакетов	Позволяет контролировать аутентичность, целостность и конфиденциальность передаваемых данных
Шифрование трафика	Обеспечивает криптографическую защиту сетевого трафика

Настройка механизма авторизации сетевых соединений осуществляется централизованно в Центре управления. Она выполняется на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров.

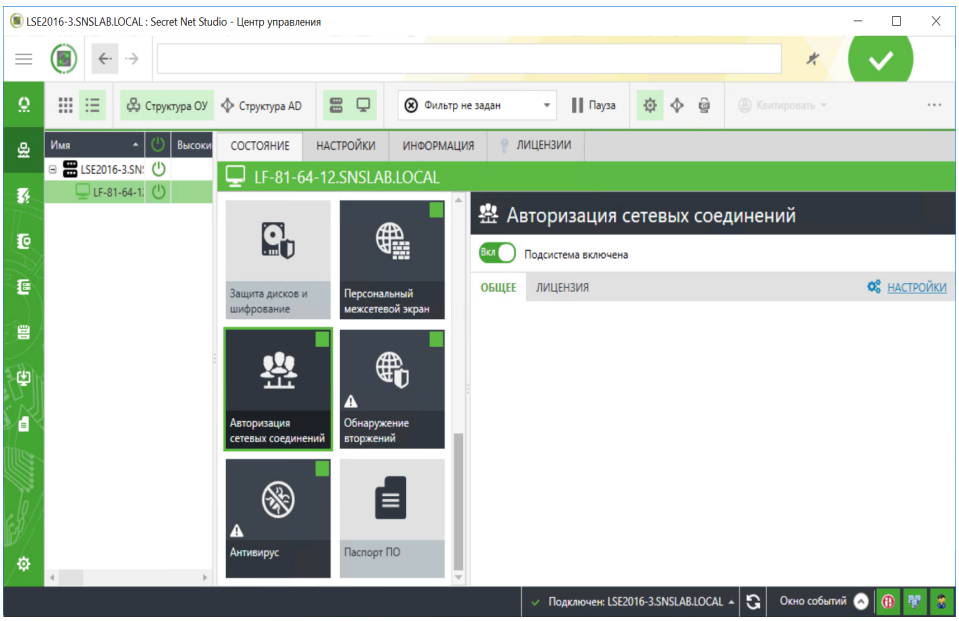
Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". С помощью данного компонента можно только посмотреть настройки механизма авторизации сетевых соединений непосредственно на защищаемом компьютере.

Внимание! Настройка механизма авторизации сетевых соединений от имени локальной учетной записи пользователя Windows не поддерживается.

Для настройки параметров:

1. Откройте Центр управления Secret Net Studio.

   На экране появится основное окно программы.



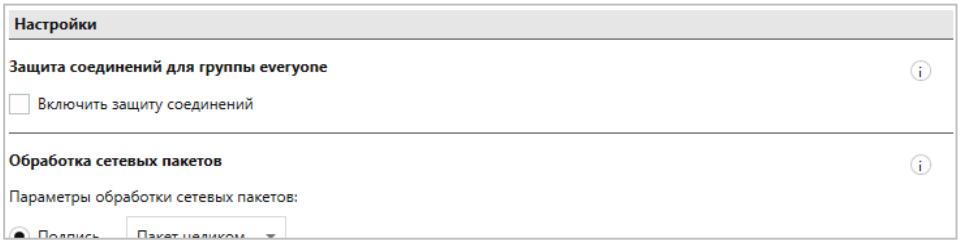
> **Совет.** Для просмотра значений параметров механизма авторизации сетевых соединений непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Авторизация сетевых соединений". В локальном режиме управления редактирование параметров недоступно.

2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

   В правой части экрана появится информация о состоянии компьютера.

3. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Авторизация сетевых соединений".

   В правой части экрана появится область настройки выбранных параметров.



4. Настройте нужные параметры и для сохранения новых значений нажмите кнопку "Применить" внизу вкладки "Настройки".

Настройка защиты соединений для группы everyone

Чтобы разрешить защиту сетевых соединений в правилах доступа, настроенных для группы everyone, отметьте поле "Включить защиту соединений" и нажмите кнопку "Применить" внизу вкладки "Настройки".

Настройка параметров обработки пакетов

В Secret Net Studio реализован механизм защиты сетевого взаимодействия между авторизованными абонентами. Данный механизм базируется на открытых стандартах протоколов семейства IPsec и обеспечивает безопасность обмена данными.

В текущей версии используются следующие протоколы.

Название	Значение
Протокол AH (Authentication Header)	Позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP-пакета. Обеспечивает защиту от атак типа "Man in the Middle"
Протокол ESP (Encapsulating Security Payload)	Используется для кодирования и контроля целостности передаваемых данных
Протокол ISAKMP	Предназначен для обмена ключами и согласования параметров соединения

Реализовано несколько режимов настройки. Администратор может для каждого защищаемого компьютера указать индивидуальный режим защиты.

По умолчанию параметры механизма авторизации сетевых соединений настроены следующим образом:

- включен режим добавления служебной информации в пакеты с уровнем анализа "Пакет целиком";
- включен режим защиты от replay-атак;
- сценарий определения пользователя SMB-соединения — от имени учетной записи пользователя.

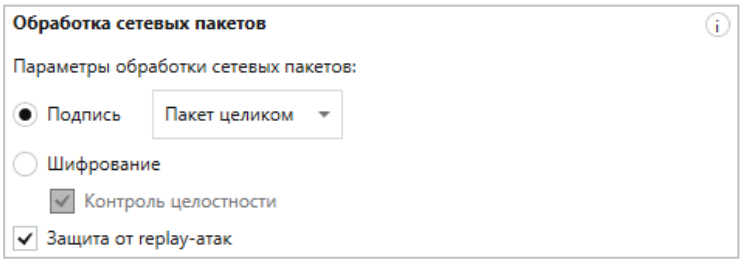
Защита и целостность передаваемых данных обеспечивается следующими средствами:

- режим добавления служебной информации в пакеты;
- режим шифрования и контроля целостности;
- режим защиты от replay-атак.

Примечание. В текущей версии Secret Net Studio одновременное использование протоколов AH и ESP не предусмотрено.

Для настройки параметров:

1. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки | Обработка сетевых пакетов".



2. Настройте параметры защиты сетевых пакетов.

Внимание! Для установления защищенного соединения необходимо:
- настроить для удаленного компьютера-получателя правила доступа, необходимые для обмена данными с компьютером-отправителем (см. стр.212);
- включить режим добавления служебной информации на компьютере-отправителе.

При невыполнении одного из этих условий установить защищенное соединение невозможно.

Поле	Значение
Подпись	Отметьте поле для включения режима добавления служебной информации к пакетам и выберите в списке уровень анализа: • "Только маркировка" — служебная информация формируется на основе первого сетевого пакета из серии, остальные пакеты получают метку принадлежности к аутентифицированной серии; • "Заголовки пакетов" — служебная информация формируется на основе заголовков пакетов; • "Пакет целиком" — служебная информация формируется для каждого пакета полностью. Будет ли добавляться служебная информация к исходящему пакету или нет, определяется параметрами безопасности удаленного компьютера — получателя IP-пакетов. Если на компьютере — получателе пакетов разрешен обмен данными с компьютером-отправителем и настроены соответствующие правила, то при включении режима добавления служебной информации к пакетам на компьютере-отправителе все пакеты, отправленные данному компьютеру-получателю, будут дополнены служебной информацией
Шифрование	Отметьте поле для включения режима кодирования данных
Контроль целостности	Поставьте отметку, чтобы включить режим контроля целостности закодированных пакетов. Если требуется отключить режим контроля целостности закодированных пакетов — удалите отметку из поля "Контроль целостности"
Защита от replay-атак	Отметьте поле для включения режима защиты, с помощью которого предотвращается пассивный захват данных и их пересылка

3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

Настройка SMB-соединения

Для определения пользователя SMB-соединения в Secret Net Studio реализовано несколько сценариев:

- пользователем соединения всегда считается учетная запись компьютера;
- пользователем соединения считается учетная запись пользователя — инициатора соединения. При этом остальным пользователям либо разрешается, либо запрещается пользоваться установленным SMB-соединением.

Деятельность всех пользователей, которым разрешается использовать SMB-соединение, осуществляется от имени пользователя — инициатора соединения. Если инициатор соединения неактивен более 30 секунд, то пользователем соединения считается следующий по порядку пользователь или сервис, которым требуется SMB-соединение.

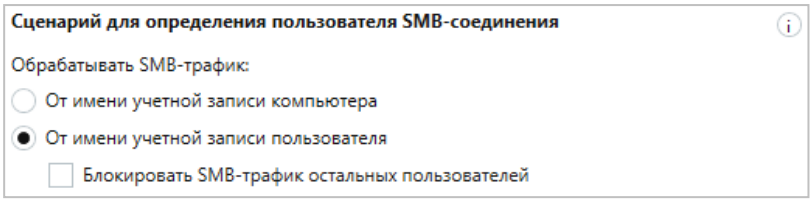
Приоритет предоставления SMB-соединений (от низшего к высшему): анонимные пользователи, сервисы, авторизованные пользователи Secret Net Studio.

При реализации сценария, при котором пользователем соединения считается инициатор соединения, остальным пользователям:

- разрешается пользоваться SMB-соединением — деятельность всех низкоприоритетных абонентов осуществляется от имени высокоприоритетного абонента;
- запрещается пользоваться SMB-соединением — при запросе SMB-соединения высокоприоритетным абонентом SMB-соединения низкоприоритетных абонентов запрещаются.

Для выбора сценария:

1. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки | Сценарий для определения пользователя SMB-соединения".



Примечание. Если SMB-соединение создается до начала работы компонентов механизма (например, mapped drive с флагом reconnect at logon), то приоритет сервисов становится равным приоритету пользователей и все дальнейшие подключения будут происходить от имени учетной записи компьютера.

2. Укажите сценарий для определения пользователя SMB-соединения.

Поле	Значение
От имени учетной записи компьютера	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью компьютера
От имени учетной записи пользователя	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью пользователя
Блокировать SMB-трафик остальных пользователей	Поставьте отметку, если требуется запретить использование SMB-соединения всем пользователям, кроме пользователя — инициатора соединения

Пояснение. Все пользователи получат доступ к объекту под одной учетной записью (первой, которая осуществила доступ на терминальный сервер) при условии, что:

- доступ к защищаемому объекту осуществляется через терминальный сервер;
- SMB-соединение устанавливается под учетной записью пользователя;
- не включен параметр "Блокировать SMB-трафик остальных пользователей".

Если параметр "Блокировать SMB-трафик остальных пользователей" включен, то доступ получит только пользователь — инициатор соединения с данным терминальным сервером.

В случае использования учетных записей компьютеров все пользователи терминального сервера получат доступ к защищаемому объекту под одной и той же учетной записью.

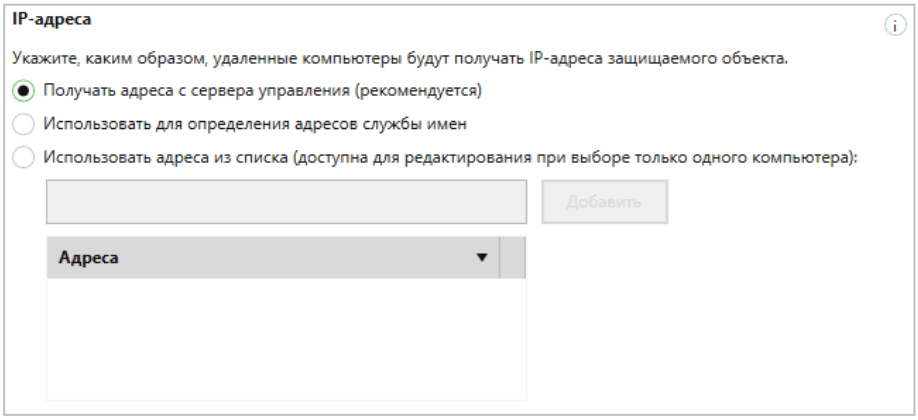
3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

Настройка параметров получения IP-адресов компьютера

Средства сетевой защиты Secret Net Studio позволяют идентифицировать компьютер не только по имени, но и по его IP-адресу. Эта возможность может быть использована, например, в случае, если имя компьютера по каким-либо причинам автоматически не преобразуется в IP-адрес.

Для настройки параметров:

1. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки | IP-адреса".



2. Настройте параметры.

Поле	Значение
Получать адреса с сервера управления	По умолчанию клиенты будут получать IP-адреса данного защищаемого компьютера автоматически с сервера безопасности, которому компьютер подчинен
Использовать для определения адресов службы имен	Отметьте это поле, чтобы за адресами клиенты обращались к службам DNS, WINS и NetBIOS
Использовать адреса из списка	Отметьте это поле, если необходимо явно задать адреса. Введите IP-адрес данного защищаемого компьютера в поле ввода и нажмите кнопку "Добавить". Если требуется удалить введенный IP-адрес, выберите его в списке и нажмите кнопку "Удалить".

3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Управление работой механизма авторизации соединений на защищаемых компьютерах

Центр управления Secret Net Studio позволяет осуществлять для отдельного компьютера управление работой механизма авторизации соединений.

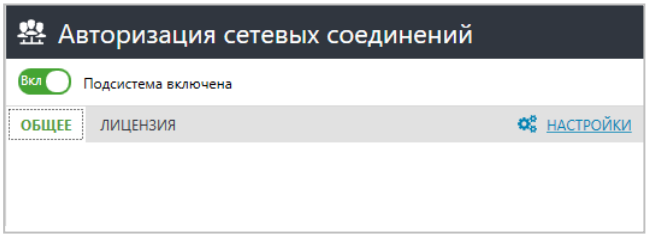
Для управления работой механизма авторизации соединений:

1. В списке объектов управления выберите нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

   На экране появится информация о состоянии данного компьютера.

2. На вкладке "Состояние" найдите и выберите объект "Авторизация сетевых соединений".

   В правой части экрана появится панель управления данным механизмом.



3. Для включения или отключения механизма переведите в нужное положение переключатель в левом верхнем углу панели.

Примечание. Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик механизма авторизации сетевых соединений (см. стр.245).

Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Глава 20
Доверенная среда

Доверенная среда Secret Net Studio является механизмом защиты, обеспечивающим внешний по отношению к ОС контроль работы ОС и системы защиты, установленных на компьютере. Контроль достигается выполнением следующих функций безопасности:

- КЦ файлов. Выполняется до загрузки ОС компьютера.
- Контроль запуска и функционирования модулей Secret Net Studio (драйверов, служб, приложений) и других драйверов. Выполняется на протяжении всего сеанса работы на компьютере.
- Блокировка от записи страниц памяти, в которых размещаются модули Secret Net Studio и другие драйверы. Обеспечивается на протяжении всего сеанса работы на компьютере.
- Обнаружение компьютерных атак, их предотвращение или аварийное завершение работы ОС компьютера при невозможности предотвращения атаки. Выполняется на протяжении всего сеанса работы на компьютере.
- Регистрация событий в журнале ДС.

Основное назначение ДС — защита информационной системы от внешнего нарушителя.

Примечание. ДС доступна в Secret Net Studio версии 8.5 и выше.

При функционирующей ДС загрузка ОС компьютера возможна только с использованием загрузочного носителя, подготовленного заранее средствами Secret Net Studio. Загрузочный носитель содержит:

- ОС ДС — специализированная ОС на базе ОС Linux, которая взаимодействует с памятью, файловой системой и ОС компьютера для реализации функций безопасности ДС;
- гипервизор ДС, обеспечивающий загрузку ОС ДС и выполнение функций безопасности ДС;
- загрузчик ДС (MBR или UEFI), предназначенный для считывания ОС ДС, гипервизора ДС и размещения их в оперативной памяти компьютера;
- настройки ДС.

Внимание! Загрузочный носитель ДС следует использовать только на доверенных АРМ.

Доверенная среда является защитным механизмом Secret Net Studio с отдельной лицензией.

Примечание. ДС является новым защитным механизмом Secret Net Studio, который находится в стадии активной разработки. Особенности настройки механизма и экранные формы могут отличаться от приведенных в данном руководстве. При возникновении вопросов по работе с ДС рекомендуется обратиться в департамент сервиса компании "Код Безопасности".

Системные требования

Требования для установки ДС Secret Net Studio приведены в таблице ниже.

Элемент	Требование
Процессор	2 ядра и более (поддерживается работа с технологией Hyper-threading). Поддержка технологии виртуализации. Для процессоров AMD Family 10h, Intel Core i3, i5, i7 и более поздних – поддержка SLAT
ОС	Все ОС, поддерживаемые Secret Net Studio, с разрядностью x64
Жесткий диск (системный)	Свободное пространство — не менее 2 МБ
Системная плата	Наличие свободного USB-разъема
UEFI/BIOS	USB-флеш-накопитель должен являться первым загрузочным устройством
USB-флеш-накопитель	Объем памяти не менее 32 МБ
Лицензия	Требуется лицензия Secret Net Studio на механизм "Доверенная среда"

Примечание. Ознакомьтесь с ограничениями и рекомендациями по использованию ДС в текущей реализации (см. стр.310).

Включение доверенной среды

Для функционирования ДС необходимо выполнить следующие действия:

- зарегистрировать лицензию на механизм ДС в Secret Net Studio;
- подготовить загрузочный носитель ДС;
- включить механизм ДС.

Регистрация лицензии на механизм ДС

Процедура регистрации лицензии на механизм ДС аналогична процедурам регистрации лицензий на другие механизмы защиты Secret Net Studio.

Лицензия может быть зарегистрирована централизованно и локально:

- при установке Secret Net Studio;
- при функционирующем Secret Net Studio.

Пояснение. После регистрации лицензии ДС по умолчанию выключена.

Регистрация при установке Secret Net Studio

Лицензия на механизм ДС может быть зарегистрирована совместно с лицензиями на другие механизмы защиты при установке Secret Net Studio. Инструкции по установке приведены в документе [**1**]:

- локальная установка — глава "Локальная установка компонентов", раздел "Установка клиента";
- централизованная установка — глава "Настройка централизованной установки клиента".

Регистрация при функционирующем Secret Net Studio

Лицензию на механизм ДС можно зарегистрировать отдельно при функционирующем Secret Net Studio. Инструкции по регистрации лицензий приведены в документе [**1**]:

- локальная регистрация — глава "Дополнительные возможности локального администрирования", раздел "Локальная регистрация лицензий";

- централизованная регистрация — глава "Настройка и контроль централизованного развертывания ПО", раздел "Управление лицензиями на использование механизмов защиты".

Создание загрузочного носителя ДС

Загрузочный носитель ДС можно создать на любом компьютере с ДС Secret Net Studio (централизованно и локально).

Совет.

- Рекомендуется создавать загрузочный носитель ДС на компьютере с типовой конфигурацией Secret Net Studio, на которой планируется использование ДС. Это связано с тем, что при создании загрузочного носителя ДС формируется список модулей Secret Net Studio, целостность которых будет контролироваться.
- Рекомендуется создавать загрузочный носитель на доверенном АРМ администратора ДС.

Создание загрузочного носителя ДС доступно и при включенной, и при выключенной ДС.

Для создания загрузочного носителя ДС необходим отдельный USB-флеш-накопитель.

Перед выполнением процедуры создания загрузочного носителя ДС подключите USB-флеш-накопитель к компьютеру.

Внимание! При создании загрузочного носителя ДС все данные на USB-флеш-накопителе уничтожаются. Создается раздел небольшого объема для служебной информации ДС; память USB-флеш-накопителя используется лишь частично. Для дальнейшего использования устройства в качестве обычного USB-флеш-накопителя и задействования всего объема памяти выполните полную очистку по инструкции со стр.312.

Ниже приведена процедура создания загрузочного носителя ДС в Локальном центре управления. В централизованном режиме процедура выполняется аналогично.

Для создания загрузочного носителя ДС:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится Центр управления Secret Net Studio в локальном режиме.

2. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда", подобные представленным на рисунке ниже.

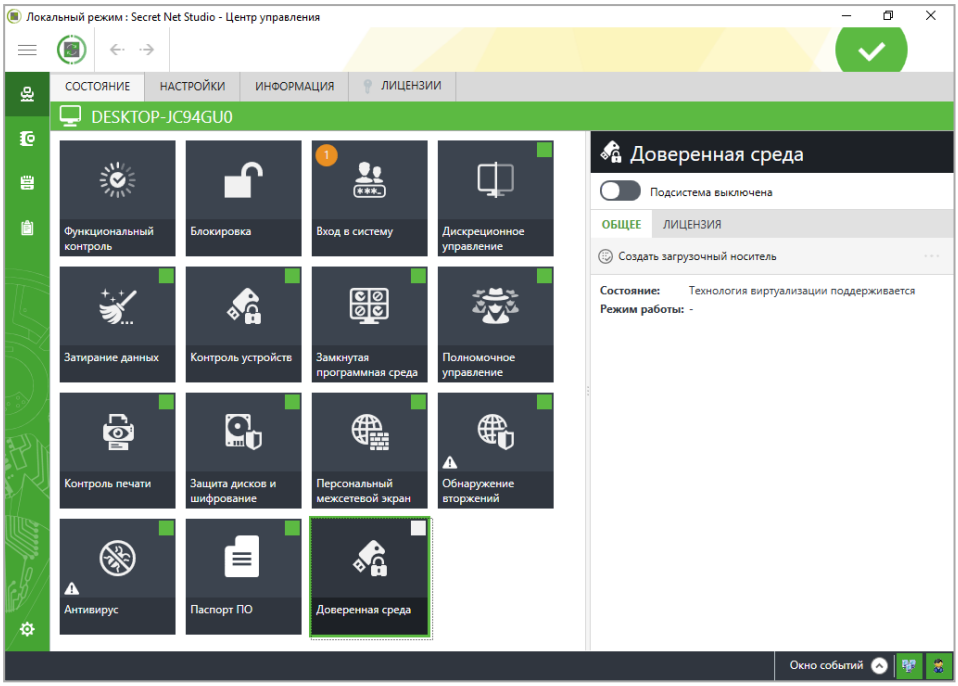
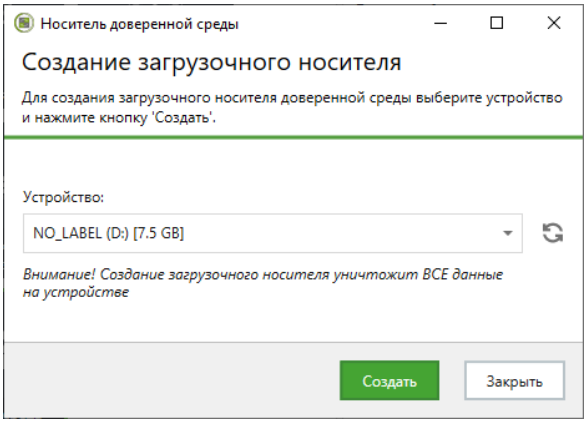


Рис.1 Сведения о подсистеме "Доверенная среда"

3. Нажмите кнопку "Создать загрузочный носитель".

   На экране появится окно создания загрузочного носителя ДС, подобное представленному на рисунке ниже.



4. Выберите подключенный USB-флеш-накопитель в раскрывающемся списке устройств.
5. Нажмите кнопку "Создать".

   Начнется процедура записи данных на USB-флеш-накопитель. По окончании процедуры в окне создания загрузочного носителя ДС появится сообщение об успешном завершении записи.
6. Нажмите кнопку "Закрыть".

   Загрузочный носитель ДС подготовлен к работе.

Включение механизма ДС

Включение механизма ДС выполняется локально на компьютере, на котором планируется использование ДС.

Внимание! Перед включением ДС Secret Net Studio убедитесь, что:

- Компьютер соответствует системным требованиям, приведенным на стр.**251**. Информация о соответствии/несоответствии отображается в программе управления в централизованном и локальном режимах работы (окно со сведениями о подсистеме "Доверенная среда" (см. Рис.1 на стр.**253**), параметр "Состояние"). Перечень возможных значений данного параметра при несоответствии компьютера системным требованиям приведен на стр.**308**.
- Подготовлен загрузочный носитель ДС (см. стр.**252**). Без него невозможно войти в ОС компьютера.

Примечание. Secret Net Studio версии 8.7 не поддерживает одновременную работу подсистемы ДС с механизмом защиты дисков и с подсистемой полнодискового шифрования. Перед включением подсистемы ДС необходимо отключить механизм защиты дисков и подсистему полнодискового шифрования.

Для включения ДС:

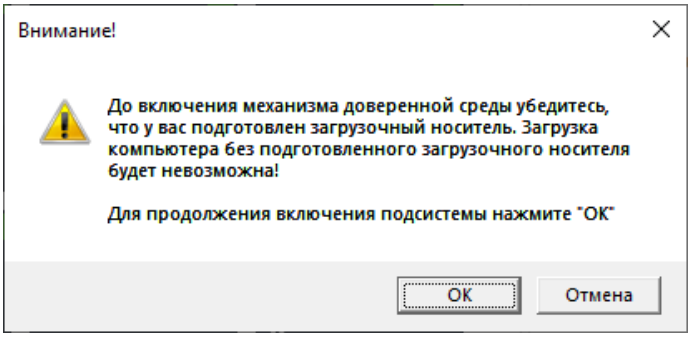
1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится Локальный центр управления Secret Net Studio. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда".

2. Переключите тумблер "Подсистема выключена" в положение "Вкл".

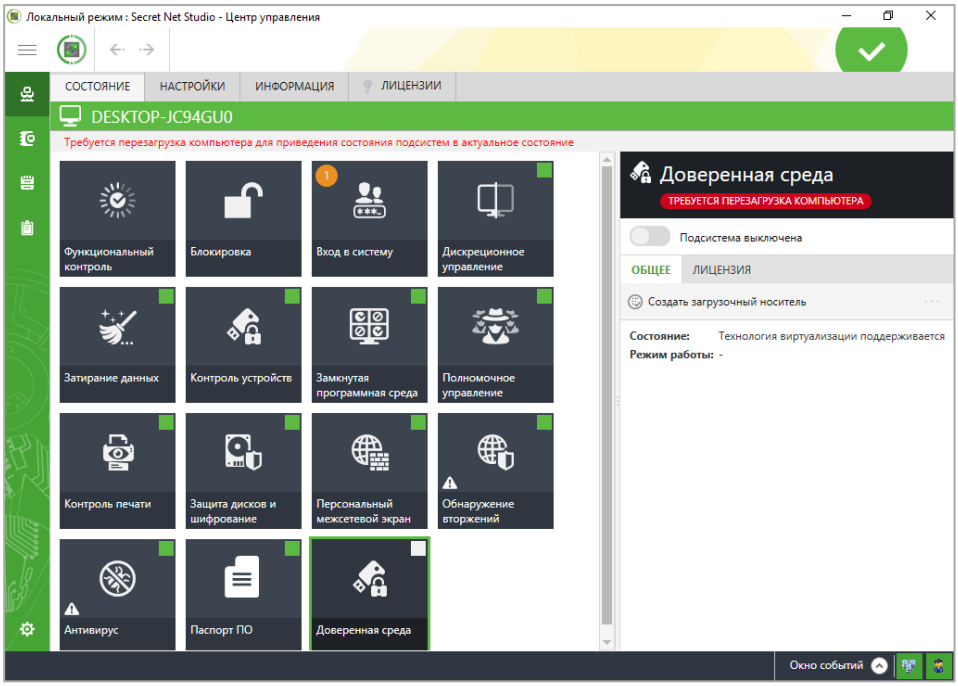
   Появится предупреждение:



3. Если загрузочный носитель ДС подготовлен, нажмите кнопку "ОК".

   Пояснение. Если загрузочный носитель ДС не подготовлен, нажмите кнопку "Отмена" и создайте его по инструкции, приведенной на стр.**252**.

   В Центре управления появится предупреждение о необходимости перезагрузки компьютера, подобное представленному на рисунке ниже.



4. Подключите загрузочный носитель ДС к компьютеру.

Внимание!
- Убедитесь, что в UEFI/BIOS первым загрузочным устройством является USB-флеш-накопитель.
- В некоторых UEFI/BIOS порядок загрузки сбивается после каждого включения компьютера. В таком случае при каждом включении компьютера нужно указывать порядок загрузки в UEFI/BIOS Setup (меню Boot).

Внимание! При включении компьютера без загрузочного носителя ДС на экране блокировки ОС компьютера появится сообщение "Ошибка выполнения функционального контроля. Причины: доверенная среда не функционирует". Вход в ОС будет невозможен.

5. Перезагрузите компьютер.

Начнется процесс загрузки ОС ДС с загрузочного носителя ДС. При успешной загрузке на экране появится меню ОС ДС (см. Рис.2 на стр.**257**).

Механизм ДС будет функционировать в мягком режиме (см. стр.**258**).

Пояснение. При невыполнении системных требований после перезагрузки могут возникнуть ошибки. В этом случае следуйте инструкциям из сообщений об ошибках.

При возникновении системной ошибки BSOD ознакомьтесь с причиной ее возникновения по коду, отображенному на экране. Возможные коды ошибок, связанных с функционированием ДС, и их описание приведены на стр.**309**.

Настройка доверенной среды

Настройка механизма ДС выполняется локально в административном режиме ДС администратором ДС.

Инструкция по входу в административный режим ДС приведена на стр.**256**.

Администратору ДС доступны следующие операции:

- выбор режима работы ДС (см. стр.**258**);
- настройка контроля целостности (см. стр.**260**);
- работа с журналом событий (см. стр.**264**);
- смена пароля администратора ДС (см. стр.**257**);
- снятие блокировки компьютера (см. стр.**263**).

Перед настройкой механизма ДС ознакомьтесь с описанием интерфейса ОС ДС и инструкциями по выполнению типовых действий (см. ниже).

Интерфейс ОС ДС

ОС ДС имеет текстовый интерфейс (см. Рис.2 на стр.**257**). Язык интерфейса — английский.

Управление осуществляется с помощью клавиатуры. Ниже приведен перечень типовых команд, знание которых упростит пользование данным руководством.

- Для навигации по пунктам меню используйте клавиши < ↑ > и < ↓ >.
- Для навигации по кнопкам в интерфейсе используйте клавиши <→> и <←>.
- Для выбора пункта меню, нажатия кнопки, выбора записи журнала и т. п. используйте клавишу <Enter>.
- Для установки отметки " * " в перечне вариантов (например, при выборе режима работы ДС) используйте клавишу <Пробел>.
- Для выхода или отмены используйте клавишу <Esc> или кнопки "Exit", "Cancel" в интерфейсе.

Вход в административный режим ДС

Внимание! Перед включением компьютера убедитесь, что:
- подключен загрузочный носитель ДС;
- в UEFI/BIOS первым загрузочным устройством является USB-флеш-накопитель.

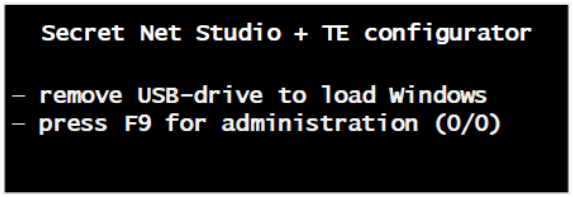
Внимание! При включении компьютера без загрузочного носителя ДС на экране блокировки ОС компьютера появится сообщение "Ошибка выполнения функционального контроля. Причины: доверенная среда не функционирует". Вход в ОС будет невозможен.

Для входа в административный режим ДС:

1. Включите компьютер.

   Начнется процесс загрузки ОС ДС с загрузочного носителя ДС.

   При успешной загрузке на экране появится меню ОС ДС:



   Пояснение.
   - При невыполнении системных требований могут возникнуть ошибки. В этом случае следуйте инструкциям из сообщений об ошибках.
   - При возникновении системной ошибки BSOD ознакомьтесь с причиной ее возникновения по коду, отображенному на экране. Возможные коды ошибок, связанных с функционированием ДС, и их описание приведены на стр.**309**.
   - При функционировании ДС в жестком режиме и возникновении событий, приводящих к остановке работы ОС (см. Табл.1 на стр.**259**), на экране появится окно с сообщением о наличии новых событий в журнале (см. Рис.5 на стр.**263**). В этом случае следуйте инструкции по снятию блокировки компьютера, приведенной на стр.**263**.

2. Нажмите клавишу <F9>.

   Пояснение. Для загрузки ОС компьютера без входа в административный режим ДС извлеките загрузочный носитель ДС.

3. Введите пароль администратора ДС.

   Внимание!
   - При первой загрузке ОС ДС пароль администратора ДС — "12345678".
   - В целях безопасности настоятельно рекомендуется сменить пароль администратора ДС после первой загрузки ОС ДС (см. стр.**257**).

На экране появится меню администратора ДС:

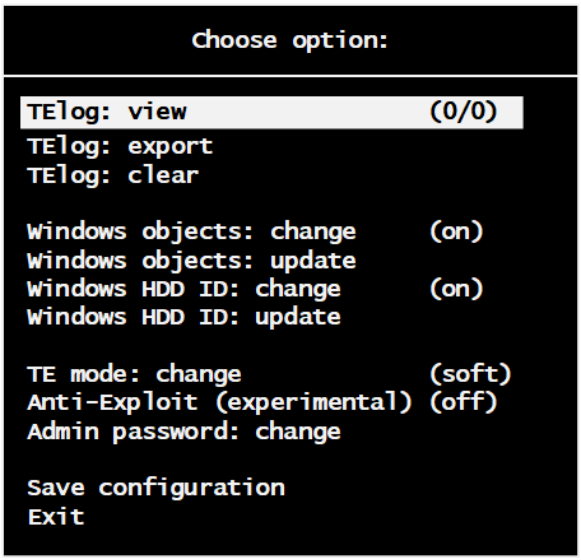


Рис.2 Меню администратора ДС

Внимание! При первом входе в административный режим ДС определяется расположение файла журнала ДС, которое необходимо сохранить. Для этого выберите в меню администратора ДС пункт "Save configuration".

4. Выберите нужный параметр для настройки:
   - TElog: view — просмотр журнала событий;
   - TElog: export — экспорт журнала событий;
   - TElog: clear — очистка журнала событий;
   - Windows objects: change — изменение перечня объектов КЦ;
   - Windows objects: update — обновление эталонных КС объектов КЦ;
   - TE mode: change — изменение режима работы ДС;
   - Admin password: change — смена пароля администратора ДС.

Пояснение. Параметры "Windows HDD ID: change" и "Windows HDD ID: update" имеются в ранних версиях Secret Net Studio с ДС. Они предназначены для оптимизации загрузки ДС при наличии нескольких разделов на жестких дисках компьютера. При установке параметра "Windows HDD ID: change" в значение "On" в конфигурации ДС сохраняется номер раздела, на котором хранится журнал ДС, и в дальнейшем загрузка выполняется сразу с нужного раздела. Параметр "Windows HDD ID: update" предназначен для обновления сведений о загрузочном разделе.
После установки пакетов обновлений указанные параметры могут отсутствовать.

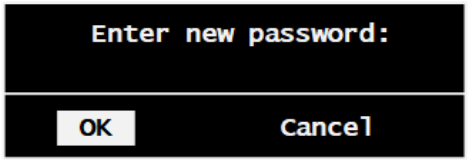
Смена пароля администратора ДС

Внимание! В целях безопасности настоятельно рекомендуется сменить пароль администратора ДС после первой загрузки ОС ДС.
Дальнейшая смена пароля администратора ДС выполняется с частотой, установленной политикой безопасности организации.

Для смены пароля администратора ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите команду "Admin password: change".

   Появится окно для ввода нового пароля:



2. Введите новый пароль.

Пояснение.

- Пароль может содержать только следующие символы:
  - 1234567890 — цифры;
  - abcdefghijklmnopqrstuvwxyz — латинские буквы нижнего регистра (строчные);
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ — латинские буквы верхнего регистра (заглавные);
  - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — специальные символы.
- Для установки стойкого пароля рекомендуется соблюдать следующие требования:
  - длина пароля должна быть не менее 6 символов;
  - пароль должен содержать хотя бы одну цифру;
  - пароль должен содержать хотя бы одну букву верхнего регистра (заглавная буква);
  - пароль должен содержать хотя бы одну букву нижнего регистра (строчная буква);
  - пароль должен содержать хотя бы один специальный символ;
  - пароль не должен содержать двух или более рядом стоящих одинаковых символов;
  - пароль не должен содержать двух или более рядом стоящих цифр, образующих возрастающую последовательность вида 123... или убывающую 987...;
  - при смене пароля новый пароль не должен совпадать с текущим.

3. Нажмите кнопку "OK".

Появится окно для подтверждения пароля:

4. Повторно введите новый пароль.
5. Нажмите кнопку "OK".

При успешном подтверждении пароля появится сообщение о смене пароля.

Пояснение. При возникновении ошибки появится сообщение "Passwords not matched". В этом случае нажмите кнопку "OK" и повторите процедуру смены пароля.

6. Нажмите кнопку "OK".
7. В меню администратора ДС выберите пункт "Save configuration".

Появится сообщение об успешном сохранении конфигурации.

8. Нажмите кнопку "OK".

Выбор режима работы ДС

ДС Secret Net Studio может функционировать в мягком и жестком режимах.

В мягком режиме ДС обеспечивает обнаружение и, если это возможно, предотвращение компьютерных атак, а также регистрацию событий безопасности в журнал событий ДС.

В жестком режиме ДС дополнительно обеспечивает остановку работы ОС компьютера при невозможности предотвращения атаки.

Особенности реакции ДС на разные типы компьютерных атак в мягком и жестком режимах работы ДС представлены в таблице ниже.

Табл.1 Особенности режимов работы ДС

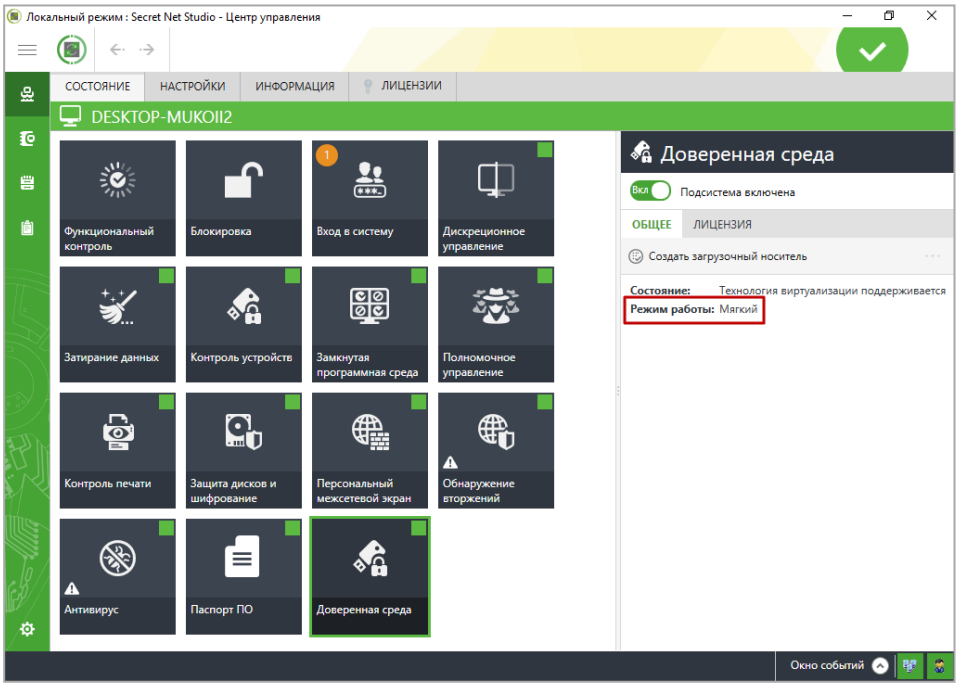
Тип атаки	Реакция ДС	
	Мягкий режим	Жесткий режим
Изменение драйверов СЗИ[1] (установка пакетов обновлений)	Обнаружение Предотвращение	Обнаружение Предотвращение
Остановка драйверов СЗИ	Обнаружение	Обнаружение Остановка ОС
Остановка процессов СЗИ[2]	Обнаружение Предотвращение	Обнаружение Предотвращение
Обнаружение вредоносного ПО[3]	Обнаружение Предотвращение	Обнаружение Предотвращение
Нарушение КС объектов КЦ	Обнаружение	Обнаружение Остановка ОС

[1] Драйвер СЗИ – драйвер Secret Net Studio, поставленный на контроль в ДС.
[2] Процесс СЗИ – процесс Secret Net Studio, который использует API ДС для защиты.
[3] Вредоносное ПО, найденное при обнаружении компьютерных атак (см. стр.**263**).

По умолчанию ДС функционирует в мягком режиме.

Текущий режим работы ДС можно посмотреть:

- в программе управления Secret Net Studio в локальном и централизованном режимах — сведения о механизме "Доверенная среда", параметр "Режим работы" (пример из Локального центра управления представлен на рисунке ниже);



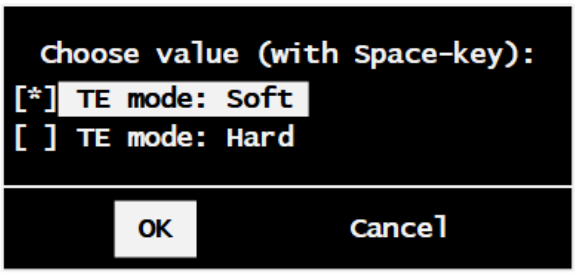
- в меню администратора ДС (см. Рис.2 на стр.**257**) — пункт "TE mode: change" (см. рисунок ниже).

Внимание! Операции обновления, исправления, удаления компонентов Secret Net Studio (в том числе пакетов обновлений) возможны только в мягком режиме работы ДС или при выключенной ДС. При попытке выполнения указанных действий в жестком режиме работы ДС появится сообщение "Для изменения или удаления программы, ее компонентов или пакетов исправлений необходимо переключить доверенную среду в мягкий режим работы".

Для смены режима работы ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите команду "TE mode: change".

   Появится окно выбора режима работы ДС:



2. Выберите нужный режим работы, установив отметку клавишей <Пробел>:
   - TE mode: Soft — для установки мягкого режима работы ДС;
   - TE mode: Hard — для установки жесткого режима работы ДС.
3. Нажмите кнопку "OK".

   Пояснение. Для отмены нажмите кнопку "Cancel".
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении изменений.
5. Нажмите кнопку "OK".

Настройка контроля целостности в ДС

Функция контроля целостности в ДС обеспечивает:

- блокировку модификации кода драйверов Secret Net Studio в памяти (в том числе с возможностью блокировки модификации кода сторонних драйверов);
- защиту от несанкционированной остановки драйверов Secret Net Studio;
- защиту от несанкционированного терминирования ключевых процессов Secret Net Studio.

При создании загрузочного носителя ДС на контроль по умолчанию ставятся критические службы и драйверы Secret Net Studio и рассчитываются их эталонные контрольные суммы (КС). Список объектов КЦ ДС по умолчанию приведен на стр.**310**.

При эксплуатации ДС можно ставить на контроль другие драйверы и файлы.

Процедуры КЦ разных объектов различаются:

- Целостность драйвера контролируется посредством проверки запуска драйвера на этапе загрузки ОС, проверки КС драйвера в памяти до исполнения его кода, блокировки памяти драйвера от записи.
- Целостность файла контролируется посредством проверки КС файла до загрузки ОС.

При нарушении целостности объектов КЦ в жестком режиме работы ДС обеспечивается остановка работы ОС компьютера. Появляется окно системной ошибки BSOD с кодом "0x5ECCODE0" (см. стр.**309**). Информация о нарушении фиксируется в журнале событий ДС.

Список объектов КЦ, созданный по умолчанию, можно редактировать:

- изменять путь к объекту КЦ (см. ниже);
- ставить на контроль/снимать с контроля выбранный объект КЦ (см. стр.**262**);
- добавлять объекты в список (см. стр.**262**);
- исключать объекты из списка (см. стр.**262**).

Внимание! После изменения списка необходимо выполнить перерасчет эталонных КС объектов КЦ (см. стр.**262**).

Для изменения пути к объекту КЦ:

1. В меню администратора ДС (см. Рис.2 на стр. **257**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ, подобное представленному на рисунке ниже.

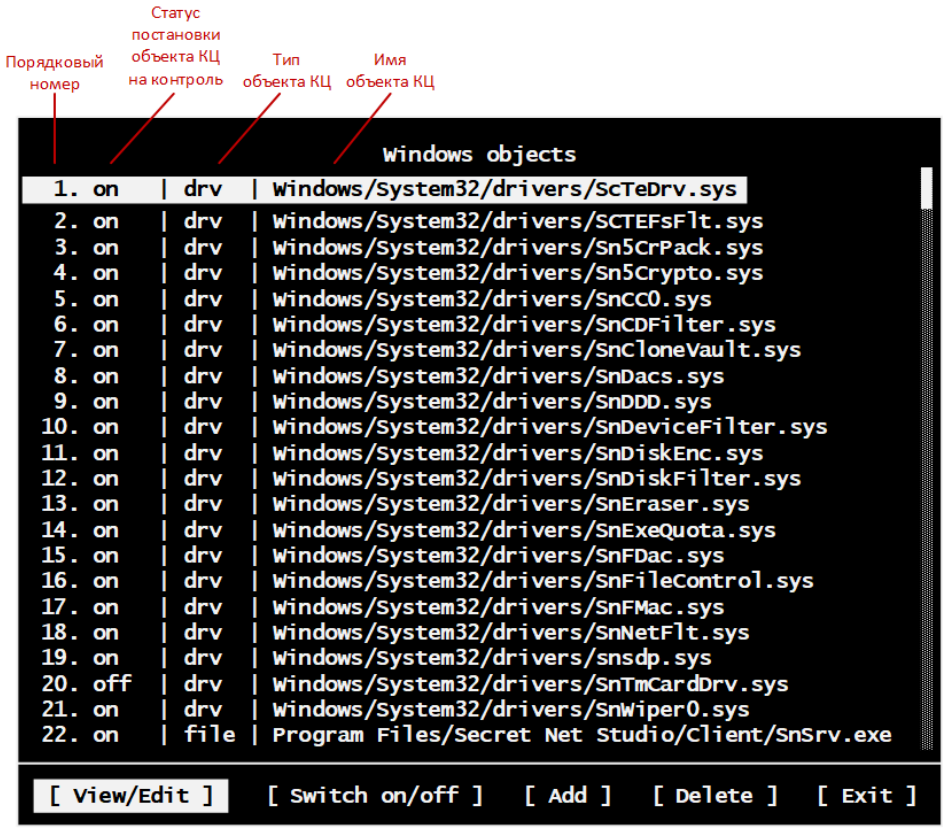


Рис.3 Окно с таблицей объектов КЦ

2. Выберите нужный объект в таблице и нажмите кнопку "[View/Edit]".

   Появится окно для изменения пути к файлу и пути к драйверу:

Рис.4 Окно изменения путей к файлу и драйверу

3. Выберите дальнейшее действие:
   - для изменения пути к файлу нажмите кнопку "[Set file path]" и внесите необходимые правки;
   - для изменения пути к драйверу нажмите кнопку "[Set driver path]" и внесите необходимые правки;
   - для возврата к таблице объектов КЦ нажмите кнопку "[OK]".
4. Нажмите кнопку "[Exit]" или клавишу <Esc>.
5. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
6. Нажмите кнопку "OK".

Для постановки на контроль/снятия с контроля объекта КЦ:

1. В меню администратора ДС (см. Рис.2 на стр. **257**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**261**).
2. Выберите нужный объект в таблице и нажмите кнопку "[Switch on/off]".

   Выбранный объект КЦ будет поставлен на контроль/снят с контроля (изменится статус "on/off" во второй колонке таблицы объектов КЦ).
3. Нажмите кнопку "[Exit]" или клавишу <Esc>.
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
5. Нажмите кнопку "OK".

Для добавления объекта в список объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр. **257**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**261**).
2. Нажмите кнопку "[Add]".

   На экране появится окно выбора объектов.
3. Выберите объект, который хотите добавить в список контролируемых.

   Пояснение. Для корректного добавления драйвера необходимо знать его внутреннее имя. Например, у драйвера SnDacs.sys внутреннее имя \Driver\SnDacs, у драйвера SnWiper0.sys – \Driver\SnWiper.
4. Нажмите клавишу <Enter>.

   Появится окно для изменения пути к файлу и пути к драйверу (см. Рис.4 на стр.**261**).
5. При необходимости измените путь к файлу/драйверу и нажмите кнопку "[OK]".

   Объект будет добавлен в список объектов КЦ ДС.
6. Нажмите кнопку "[Exit]" или клавишу <Esc>.
7. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
8. Нажмите кнопку "OK".

Для удаления объекта из списка объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр. **257**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**261**).
2. Выберите нужный объект в таблице и нажмите кнопку "[Delete]".

   Объект будет удален из списка.
3. Нажмите кнопку "[Exit]" или клавишу <Esc>.
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
5. Нажмите кнопку "OK".

Для перерасчета эталонных КС объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр. **257**) выберите команду "Windows objects: update".

   Появится сообщение об успешном выполнении операции.
2. Нажмите кнопку "OK".
3. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.

4. Нажмите кнопку "OK".

Настройка обнаружения компьютерных атак

Примечание. Функция обнаружения компьютерных атак в ДС Secret Net Studio (Anti-Exploit) на данном этапе является экспериментальной. По умолчанию данная функция отключена.

ДС Secret Net Studio обеспечивает обнаружение следующих видов компьютерных атак:

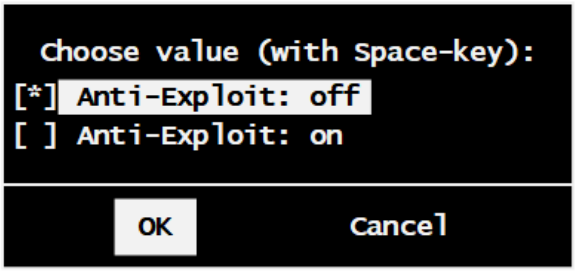
- сброс SMEP;
- выполнение команд в стеке;
- эксплуатация уязвимости EternalBlue;
- запись данных в защищаемую область памяти.

При обнаружении атаки ДС обеспечивает их предотвращение или остановку работы ОС компьютера в зависимости от типа атаки (см. Табл.1 на стр.**259**). Информация об атаке фиксируется в журнале событий ДС.

Для включения/выключения функции обнаружения атак:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите команду "Anti-Exploit (experimental)".

   Появится окно настройки функции обнаружения атак:



2. Выберите нужный вариант, установив отметку клавишей <Пробел>:
   - Anti-Exploit: off — для выключения функции обнаружения атак;
   - Anti-Exploit: on — для включения функции обнаружения атак.
3. Нажмите кнопку "OK".

   Пояснение. Для отмены нажмите кнопку "Cancel".
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном выполнении операции.
5. Нажмите кнопку "OK".

Снятие блокировки компьютера

В жестком режиме работы ДС при возникновении определенных событий (см. Табл.1 на стр.**259**) останавливается работа ОС и компьютер блокируется. В этом случае при включении компьютера появляется сообщение о наличии в журнале новых событий, подобное представленному на рисунке ниже.

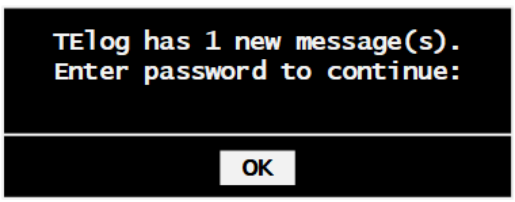


Рис.5 Сообщение о наличии новых событий (жесткий режим работы ДС)

Без просмотра администратором ДС журнала событий невозможно загрузить ОС компьютера.

Для снятия блокировки компьютера:

1. В окне с сообщением о наличии новых событий введите пароль администратора ДС и нажмите кнопку "OK".

   На экране появится окно журнала событий ДС (см. Рис.6 на стр.**265**).

2. Просмотрите подробную информацию о событии, которое привело к блокировке компьютера. Данное событие имеет статус "New".

   Пояснение. Может быть несколько событий, которые привели к блокировке компьютера. Для снятия блокировки просмотрите информацию обо всех новых событиях.

   Внимание! По факту произошедшего события произведите административные действия, установленные политикой безопасности организации для событий такого типа.

3. Закройте журнал событий, нажав кнопку "[Exit]" или клавишу <Esc>.

   На экране появится меню администратора ДС (см. Рис.2 на стр.**257**).

4. Выберите пункт "Exit".

   Компьютер разблокирован и готов к загрузке штатной ОС.

Работа с журналом событий

В ДС регистрируются следующие типы событий:

- попытка несанкционированной остановки служб Secret Net Studio;
- попытка выгрузки драйверов Secret Net Studio;
- нарушение целостности объектов КЦ;
- попытка модификации кода драйверов Secret Net Studio;
- ошибка при входе в административный режим ДС.

Журнал событий ДС хранится на системном диске.

Журнал событий ДС позволяет хранить не более 4096 записей. Журнал имеет свойство перезаписи — при максимальном заполнении журнала на место устаревших событий записываются новые.

При работе с журналом администратору ДС доступны следующие операции:

- просмотр журнала, в том числе просмотр подробной информации о каждом событии;
- очистка журнала;
- экспорт журнала в файл на загрузочный носитель ДС.

Просмотр

Журнал событий ДС можно просмотреть в ОС ДС (см. инструкцию ниже) и в программе управления Secret Net Studio.

Для просмотра журнала в программе управления необходимо предварительно экспортировать журнал в файл на загрузочный носитель ДС средствами ДС (см. стр.**266**). Инструкция по загрузке экспортированного журнала в Центр управления приведена в документе [**1**] (глава "Работа с централизованными журналами", раздел "Загрузка записей журналов").

Для просмотра журнала событий в ОС ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите команду "TElog: view".

   Появится окно журнала событий, подобное представленному на рисунке.

Рис.6 Журнал событий ДС

Пояснение. Если журнал событий пуст, на экране появится сообщение "TElog is empty".

2. Выполните нужное действие:

- Для навигации по событиям используйте клавиши < ↑ > и < ↓ >.
- Для просмотра подробной информации о выбранном событии нажмите кнопку "[Select]". Появится окно, подобное представленному на рисунке ниже.

Для возврата к окну журнала событий нажмите кнопку "[OK]".

Примечание. Событие перестает быть новым (теряет статус "New") после просмотра подробной информации о нем. Это необходимо для разблокировки компьютера в жестком режиме работы ДС (см. стр.263).

- Для удаления выбранного события нажмите кнопку "[Delete]" в окне журнала событий или в окне с подробной информацией о событии.
- Для возврата в меню администратора ДС нажмите кнопку "[Exit]".

Очистка

Внимание! Прежде чем выполнить очистку журнала, ознакомьтесь с его содержимым. Имеется возможность сохранить журнал в файл (см. ниже).

Для очистки журнала событий:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите пункт "TElog: clear" или в окне просмотра журнала событий (см. Рис.6 на стр.**265**) нажмите кнопку "[Clear TElog]".

   Журнал будет очищен. На экране появится сообщение об успешном выполнении операции.
2. Нажмите кнопку "ОК".

Экспорт

Для экспорта журнала событий:

1. В меню администратора ДС (см. Рис.2 на стр.**257**) выберите пункт "TElog: export".

   Журнал будет сохранен в файл "te.snlog" на загрузочный носитель ДС.

   На экране появится сообщение об успешном экспорте журнала в файл.
2. Нажмите кнопку "ОК".

Выключение доверенной среды

Выключение ДС выполняется локально на компьютере, на котором она функционирует.

Внимание! Выключение ДС возможно только при ее функционировании в мягком режиме (см. стр.**258**).

Для выключения ДС:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится Локальный центр управления Secret Net Studio.
2. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда".
3. Переключите тумблер "Подсистема включена" в положение "Выкл".

   В программе управления появится предупреждение о необходимости перезагрузки компьютера.
4. Извлеките загрузочный носитель ДС.
5. Перезагрузите компьютер.

   Доверенная среда будет выключена. Загрузка ОС выполнится в стандартном режиме.

Глава 21
Безопасная среда

Безопасная среда является механизмом защиты, позволяющим предотвратить нанесение ущерба ресурсам защищаемого компьютера путем запуска неизвестного программного обеспечения в изолированной среде. Механизм анализирует работу программы, определяет уровень доверия и на его основании добавляет программу в список доверенных либо в список запрещенных. Запуск неизвестного ПО может выполняться пользователями и администраторами.

Внимание! Для функционирования безопасной среды требуется ОС Windows 11 или Windows 10.

Примечание. Безопасная среда доступна в Secret Net Studio версии 8.7 и выше.

Включение механизма

Включение механизма "Безопасная среда" на защищаемых компьютерах может выполняться автоматически или вручную. Автоматическое включение происходит при централизованной установке клиента после регистрации лицензии в централизованном хранилище (по умолчанию в задании развертывания механизм отмечен для установки).

Если лицензия для механизма "Безопасная среда" зарегистрирована на компьютере после установки клиента, включение механизма необходимо выполнить вручную централизованно или локально.

Внимание! Безопасная среда не поддерживает работу при включенном жестком режиме ЗПС, а также при включенном режиме контроля потоков.

Ниже приводится описание процедуры включения механизма "Безопасная среда" при работе с Центром управления. Включение механизма локально выполняется аналогично с использованием Локального центра управления.

Для централизованного включения механизма:

1. Откройте панель "Компьютеры", выберите нужный компьютер, вызовите его контекстное меню и выберите команду "Свойства". В появившейся панели свойств на вкладке "Состояние" нажмите плитку "Безопасная среда". Справа от плитки появится блок, содержащий сведения о механизме.
2. Переведите в положение "Вкл" выключатель, расположенный слева в заголовке блока.

Анализ программ и формирование списков

Администратор может запускать анализ программ в БС для определения уровня доверия программы, либо вручную добавлять программы в черный и белый списки. Дополнительно анализ программ может быть запущен пользователем.

Для запуска программы в безопасной среде:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Безопасная среда".
2. Перейдите на панель "Сессии" и нажмите кнопку "Запустить".

   На экране появится диалог настройки параметров сессии БС.
3. Укажите путь к программе, которую нужно проанализировать, настройте параметры сессии и нажмите кнопку "Запустить".

   Программа запускается в безопасной среде в новом контейнере для анализа или в одном из существующих.
4. Выполните все необходимые операции в анализируемой программе и закройте ее. По завершении работы с программой на экране появится диалог с результатами анализа:

- если программа достигает необходимого уровня доверия, то БС добавляет ее в белый список;
- если программа не достигает необходимого уровня доверия, то БС принудительно завершает работу программы, добавляет ее в черный список и оповещает об этом пользователя;
- если пользователь завершает работу программы раньше, чем БС закончит ее анализировать, БС сохраняет контекст анализа программы и использует его при следующем запуске программы в том же контейнере БС.

Примечание. Анализ также можно запустить через контекстное меню выбранной программы.

Для добавления программы в черный/белый список:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Безопасная среда".
2. Перейдите на панель "Списки", выберите вкладку с нужным списком и нажмите кнопку "Добавить".

   На экране появится диалог добавления программ.
3. Укажите путь к программе, которую нужно добавить в список, и нажмите кнопку "Добавить".

   Указанная программа добавится в выбранный список.

Работа с правилами

Администратор может создавать новые правила и наборы правил, редактировать существующие и удалять лишние. Все операции с правилами выполняются в программе "Безопасная среда".

Для создания набора правил БС:

1. В программе "Безопасная среда" перейдите на панель "Правила" и нажмите кнопку "Создать новый".

   На экране появится диалог создания набора правил.
2. Введите название нового набора, при необходимости выберите шаблон и нажмите кнопку "Создать".

   Указанный набор правил добавится в список наборов.

Для добавления правила БС в набор:

1. В программе "Безопасная среда" перейдите на панель "Правила", выберите набор, в который нужно добавить правило, в выпадающем списке и нажмите кнопку "Создать".

   На экране появится диалог создания правила.
2. Выберите категорию и тип правила, укажите название объекта и настройте параметры правила ("Виртуализировать" для правил доступа к файлам, "Протокол" для правил доступа к сети и т. п.).
3. Укажите необходимые значения параметров для перечня действий, отображаемого в зависимости от выбранного типа правил.

   Примечание. Параметры действий разделены на две группы: "Запрос прав" и "Выполнение". Параметры "Вес" и "Включить аудит действия" настраиваются отдельно для каждой группы.

   Параметр "Включить аудит действия" можно включить для всех правил в колонке, нажав на заголовок колонки.

   Параметр "Вес" может быть задан для набора правил и для каждого действия в каждом правиле отдельно. Если при анализе программы суммарный вес выполненных действий превысит значение, заданное для набора правил, программа будет добавлена в черный список.

   Нажмите кнопку "Добавить".

   Указанное правило добавится в выбранный набор. Для копирования уже существующего в наборе правила, выберите правило, которое нужно копировать и нажмите кнопку "Дублировать".
4. Нажмите кнопку "Сохранить".

Для редактирования правила БС в наборе:

1. В программе "Безопасная среда" перейдите на панель "Правила", в выпадающем списке выберите набор правил, в котором находится правило, требующее редактирования и дважды нажмите левую кнопку мыши.

   На экране появится диалог редактирования правила.
2. Измените параметры правила и нажмите кнопку "Применить".
3. Нажмите кнопку "Сохранить".

Для удаления набора правил БС:

- В программе "Безопасная среда" перейдите на панель "Правила", выберите набор правил, который нужно удалить, в выпадающем списке и нажмите кнопку "Удалить", находящуюся справа от списка наборов.

Для удаления правил из набора:

1. В программе "Безопасная среда" перейдите на панель "Правила", выберите набор правил, в котором находится правило, требующее удаления, выберите правило в списке и нажмите кнопку "Удалить", находящуюся над списком правил. Для выбора нескольких правил используйте вместе с мышью клавиши "Shift" и "Ctrl".

   На экране появится диалог удаления правил.
2. Нажмите кнопку "Подтвердить".

   Выбранные правила удалятся из набора.
3. Нажмите кнопку "Сохранить".

Работа с журналами

Программа "Безопасная среда" содержит собственные журналы событий. Для каждой сессии создается отдельный журнал, в котором регистрируются действия с включенным параметром аудита в правилах. Журналом управляет администратор. Доступны команды очистки и экспорта журнала.

Обновление базы правил безопасной среды

Обновление базы правил БС выполняется одними средствами с обновлением баз Антивируса и СОВ. Дополнительную информацию по обновлению баз указанных компонентов см. на стр.**1**.

Приложение

Программа управления пользователями

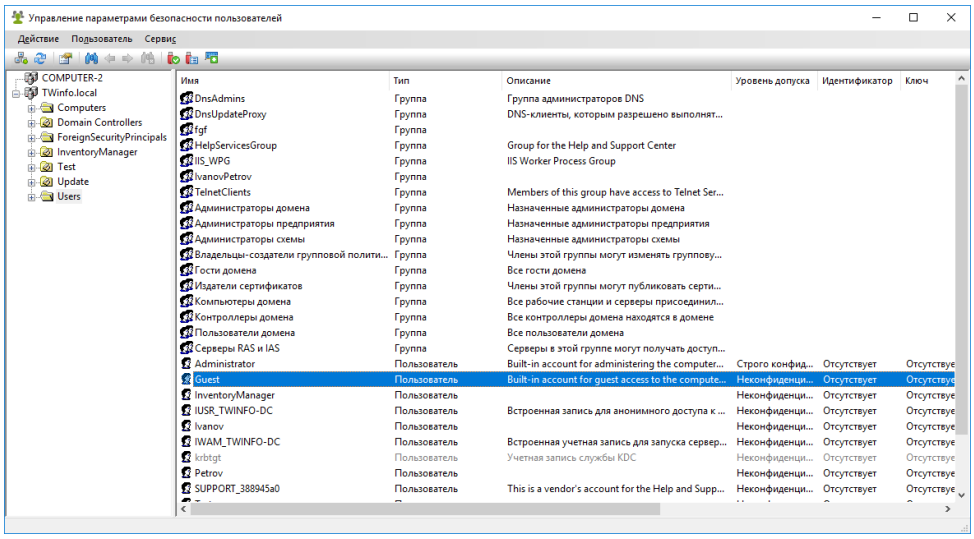
Программа управления пользователями, входящая в состав средств системы Secret Net Studio, предназначена для настройки параметров работы пользователей в системе защиты. В программе можно выполнять действия как с доменными пользователями, так и с локальными.

Для запуска программы:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Управление пользователями".

> **Внимание!** Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.
> - Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
> - Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

Пример содержимого окна программы представлен на рисунке ниже.



Интерфейс программы реализован аналогично стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры". В левой части окна отображается список контейнеров (текущий компьютер и структура разделов и организационных подразделений домена), а в правой — список пользователей в выбранном контейнере. Список пользователей представлен в виде таблицы со сведениями об уровнях допуска пользователей, наличии идентификаторов и криптографических ключей.

Если выбран параметр "Усиленная аутентификация по паролю", то для выполнения операций с пользователями необходимо будет выставлять отметку в поле "Синхронизировать данные пользователя на сервере аутентификации" при каждой операции либо выставить отметку в поле "Доверять аутентификации Windows" в Центре управления.

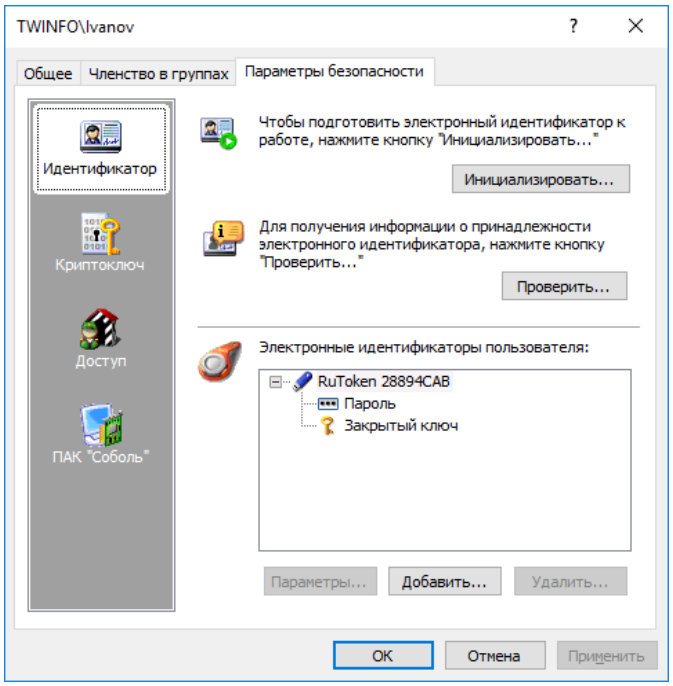
Для централизованного управления по умолчанию в программу загружается структура текущего домена. При необходимости можно загрузить структуры других доменов AD, если есть возможность подключения к этим доменам. Для этого используйте команду "Подключиться к домену Active Directory" в меню "Действие".

Совет. При работе с большим количеством объектов удобно использовать функции сортировки и поиска пользователей. Сортировка выполняется стандартными способами по содержимому колонок таблицы в списке пользователей. Поиск можно выполнять по различным критериям. Для настройки параметров поиска выберите команду "Поиск" в меню "Пользователь" и укажите нужные критерии в диалоге настройки. Результаты поиска выводятся в самом диалоге настройки, а также выделяются в списках пользователей после закрытия диалога. Для переходов между найденными объектами используйте команды "Следующий" и "Предыдущий" в меню "Пользователь".

Имеется возможность удаления из баз данных сервера аутентификации Secret Net Studio учетных записей пользователей, удаленных из AD, но оставшихся в базах Secret Net Studio. Для этого в меню "Сервис" выберите команду "Удаление потерянных пользователей".

Совет. Не рекомендуется удалять потерянных пользователей без крайней необходимости, в особенности в структуре с несколькими доменами AD (во избежание удаления пользователей из других доменов).

Управление параметрами пользователей для работы в системе Secret Net Studio осуществляется в диалоге "Параметры безопасности". Пример диалогового окна настройки свойств доменного пользователя представлен на следующем рисунке.



Использование TCP-портов для сетевых соединений

Некоторые модули системы Secret Net Studio используют определенные TCP-порты для сетевого взаимодействия. При установке клиентского ПО системы защиты на компьютере автоматически изменяются следующие параметры ОС Windows:

1. Разрешаются RPC-вызовы от неаутентифицированных клиентов. Для этого в ключе реестра HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC создается параметр RestrictRemoteClients с нулевым значением.
2. Разрешаются анонимные соединения с именованным каналом. Для этого в ключе HKLM\System\CurrentControlSet\Services\LanManServer\Parameters создается параметр NullSessionPipes со значениями SnIcheckSrv и SnHwSrv.

Дополнительно в брандмауэре Windows необходимо разрешить использование следующих TCP-портов:

- 21326 — для работы с электронными идентификаторами при терминальном доступе;
- 21327 — для оперативной синхронизации централизованно заданных заданий КЦ-ЗПС.

Перечисленные изменения достаточны для сетевого взаимодействия с использованием транспорта TCP. Также предусмотрена альтернативная возможность установления связи через именованные каналы — для этого в брандмауэре Windows необходимо вручную включить действие стандартных правил "Общий доступ к файлам и принтерам", разрешающих использование портов 139 и 445.

Необходимым условием установления соединения является разрешение использования портов 137 и 138 на защищаемых компьютерах. Данные порты открыты по умолчанию в операционной системе. В случае блокировки соединений проверьте состояние стандартных правил брандмауэра Windows, разрешающих использование указанных портов, и при необходимости включите их действие.

Устройства, контролирующие сетевой трафик между компьютерами, не должны блокировать использование перечисленных портов.

Список групп, классов и моделей для контроля устройств

Табл.2 Группы, классы и модели устройств

Группа	Класс	Модель
Локальные устройства	Последовательные порты. Параллельные порты. Сменные диски. Оптические диски. Физические диски. Процессоры. Оперативная память. Системная плата. Аппаратная поддержка. Программно реализованные диски	—

Группа	Класс	Модель
Устройства USB	Сетевые платы и модемы. Интерфейсные устройства (мышь, клавиатура, ИБП и др). Сканеры и цифровые фотоаппараты. Принтеры. Устройства хранения. Bluetooth адаптеры. Сотовые телефоны (смартфоны, КПК). Электронные идентификаторы и считыватели. Прочие	Предусмотрено создание моделей. Имеются предопределенные модели поддерживаемых электронных идентификаторов
Устройства PCMCIA	Последовательные порты и модемы. Параллельные порты. Устройства хранения. Сетевые платы. Прочие	Предусмотрено создание моделей
Устройства IEEE1394	Устройства хранения. Принтеры. Сканеры и цифровые фотоаппараты. Сетевые устройства. Цифровые видеокамеры. Прочие	Предусмотрено создание моделей
Устройства SD	Карты памяти	Предусмотрено создание моделей
Сеть	Соединение Ethernet. Беспроводное соединение (WiFi). Соединение Bluetooth. Соединение 1394 (FireWire). Инфракрасное соединение (IrDA)	Предусмотрено создание моделей для соединения 1394 (FireWire)

Примеры настройки использования подключаемых съемных дисков

Локальное присвоение пользователям определенных съемных дисков

В данном разделе рассматривается пример локальной настройки системы защиты для разграничения доступа пользователей к устройствам, которые подключаются в качестве съемных дисков. В результате настройки пользователям будут предоставлены возможности подключать и использовать определенные устройства (для каждого пользователя — отдельный съемный диск или несколько дисков), к которым другие пользователи не будут иметь доступа.

1. Подключите устройство.

   Примечание. Подключение требуется, чтобы устройство появилось в списке устройств локальной политики. Если устройство до этого уже подключалось и сведения о нем присутствуют в списке устройств, подключать устройство не обязательно.

2. Запустите Локальный центр управления. Для этого в меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".
3. В программе управления откройте панель "Компьютер" и перейдите на вкладку "Настройки".
4. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Устройства".
5. Выберите строку с подключенным устройством.
6. В ячейке колонки "Параметры контроля" удалите отметку из поля "Наследовать настройки контроля от родительского объекта" (если отметка установлена) и отметьте режим контроля "Подключение устройства разрешено".
7. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.

   На экране появится диалог ОС Windows "Разрешения...".
8. Отредактируйте список учетных записей в верхней части диалога: добавьте учетную запись пользователя, которому будет разрешено использование устройства, и удалите ненужные элементы.
9. Укажите параметры доступа для элементов списка: включите разрешения на выполнение операций для учетной записи пользователя, которому будет разрешено использование устройства, и запреты для других элементов (если они присутствуют в списке).
10. Закройте диалоги с сохранением изменений и при необходимости повторите процедуру для других устройств.
11. Нажмите кнопку "Применить" в нижней части вкладки "Настройки".

Централизованное формирование списка используемых съемных дисков

Система защиты позволяет ограничить подключение устройств (в том числе подключаемых съемных дисков) и разрешить использование только того оборудования, которое указано администратором безопасности. Для этих целей могут применяться следующие методы:

- метод формирования списка устройств на отдельном компьютере (см. стр.**84**);
- метод централизованного формирования списка используемых устройств в групповых политиках (доменов, организационных подразделений или сервера безопасности).

Если устройства преимущественно подключаются к одним и тем же компьютерам, для формирования списков устройств рекомендуется использовать первый метод. Для случаев, когда требуется составить единый список подключаемых устройств для компьютеров домена, организационного подразделения или подчиненных серверу безопасности, можно использовать средства соответствующей групповой политики в программе управления. Однако не следует помещать в такой список слишком много устройств (несколько сотен и более), так как это может привести к длительным задержкам при обновлении групповых политик на компьютерах.

Формирование списка подключаемых устройств в групповой политике осуществляется следующим образом:

1. Задайте политику контроля устройств в нужной групповой политике (см. стр.**87**).
2. В список устройств групповой политики добавьте нужные устройства (см. стр.**87**).
3. Для добавленных устройств включите режим контроля "Подключение устройства разрешено". В параметрах моделей и/или классов, к которым принадлежат добавленные устройства, включите режим контроля "Подключение устройства запрещено". Описание процедуры настройки политики контроля устройств см. на стр.**94**.

Общие сведения о программе "Контроль программ и данных"

Программа "Контроль программ и данных" предназначена для настройки механизмов КЦ и ЗПС. В ходе настройки для механизма КЦ определяются списки контролируемых объектов, методы и расписание проведения контроля, реакция системы на результат контроля. Для ЗПС определяются списки программ, запуск которых разрешен пользователям. Из этих сведений формируется модель данных, представляющая собой иерархию объектов и описание связей между ними.

Для работы с программой предусмотрены следующие режимы:

- локальный режим работы — используется для редактирования локальной модели данных на компьютере;
- централизованный режим работы — используется для редактирования централизованной модели данных с описаниями объектов, контролируемых на защищаемых компьютерах. Централизованная модель данных применяется на клиентах в сетевом режиме функционирования совместно с локальными моделями, если они заданы. При этом приоритет имеют параметры централизованной модели.

При централизованном управлении, если в системе присутствуют компьютеры с версиями ОС различной разрядности, формируются две модели данных — для компьютеров с 32-разрядными ОС и для компьютеров с 64-разрядными ОС. Администратор с помощью программы может редактировать только одну централизованную модель данных, разрядность которой совпадает с разрядностью версии ОС Windows компьютера администратора. Поэтому при необходимости редактирования централизованной модели другой разрядности администратору следует использовать компьютер с версией ОС той же разрядности.

Запуск программы

Для запуска программы в централизованном режиме:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Контроль программ и данных (централизованный режим)".

   При запуске программа проверяет возможность полного доступа к модели данных соответствующей разрядности в ЦБД КЦ-ЗПС. Полный доступ возможен только с одного компьютера системы.

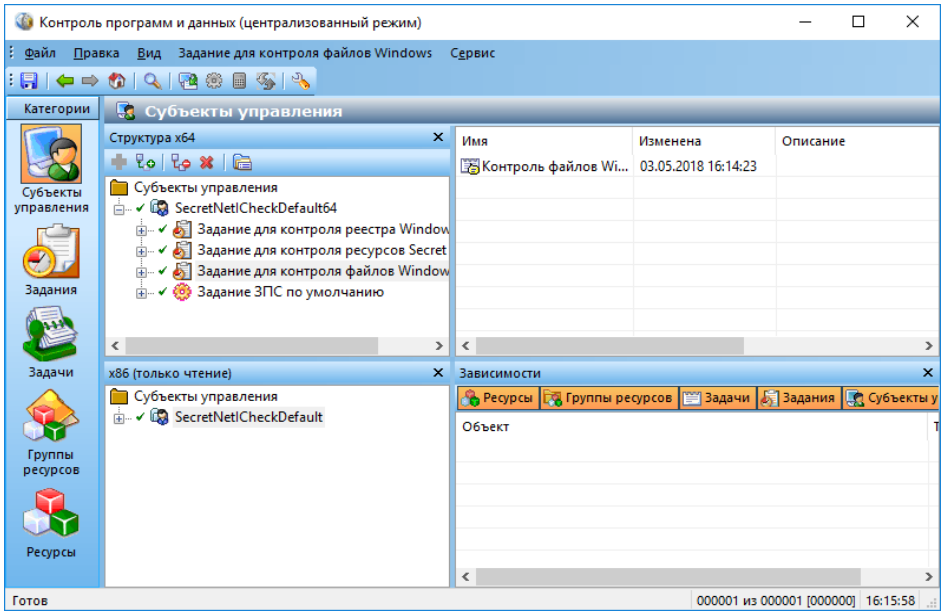
2. Если возможность полного доступа к ЦБД отсутствует (на другом компьютере с ОС той же разрядности уже работает Центр управления КЦ-ЗПС в централизованном режиме), на экране появится сообщение об этом с запросом дальнейших действий. Предусмотрены следующие варианты:

   - отменить запуск программы (рекомендуется) — для этого нажмите кнопку "Отмена";
   - запустить программу с доступом к ЦБД КЦ-ЗПС в режиме "только для чтения" — для этого нажмите кнопку "Нет". В этом случае в программу будет загружена последняя сохраненная в ЦБД модель данных. Возможность редактирования модели будет отсутствовать;
   - запустить программу и получить полный доступ к ЦБД — для этого нажмите кнопку "Да". Это приведет к тому, что пользователь, работающий с программой управления КЦ-ЗПС на другом компьютере, потеряет возможность записи в ЦБД и сохранения сделанных изменений.

Внимание! Если включена функция контроля административных привилегий, на экране появится запрос PIN администратора.

- Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
- Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

На рисунке представлен пример содержимого окна программы в централизованном режиме.



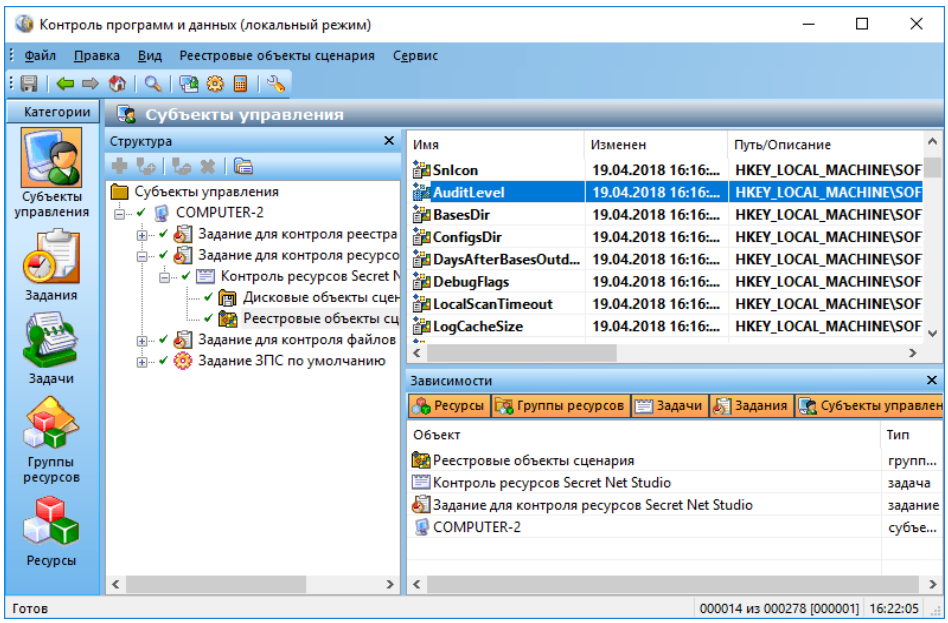
Для запуска Локального центра управления:

- В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Контроль программ и данных".

  Внимание! Если включена функция контроля административных привилегий (см. стр.44), на экране появится запрос PIN администратора.

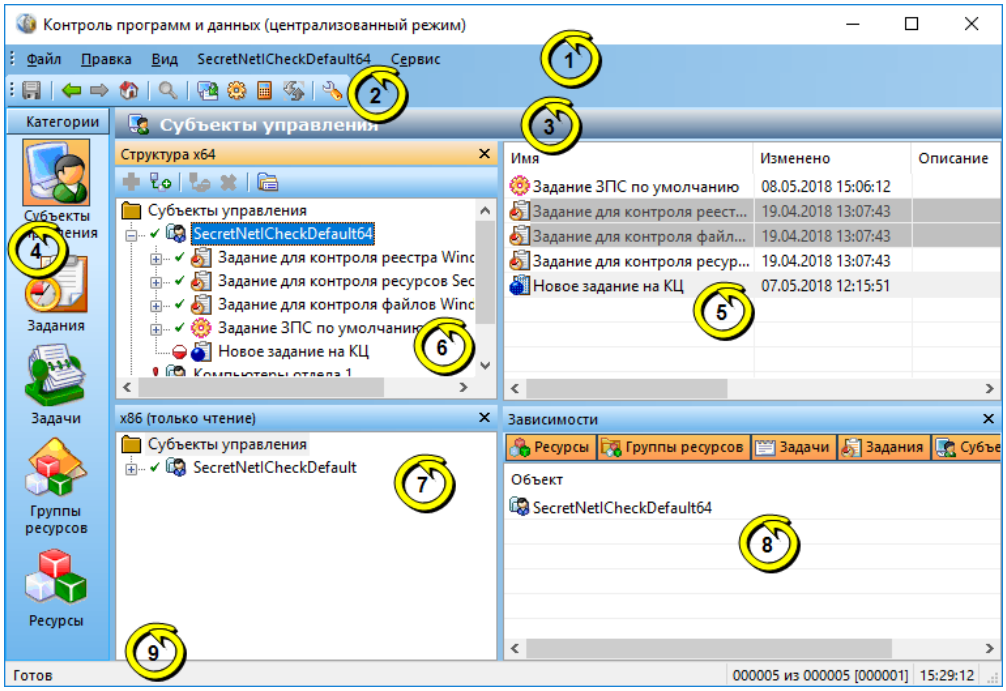
  - Для запуска программы в режиме администрирования введите PIN администратора безопасности и нажмите кнопку "ОК".
  - Для запуска программы в режиме ограниченной функциональности нажмите кнопку "Отмена" или закройте окно запроса PIN администратора.

На рисунке представлен пример содержимого окна Локального центра управления.



Интерфейс программы

При заданной по умолчанию настройке интерфейса основное окно программы управления выглядит следующим образом:



На рисунке представлен пример основного окна программы в централизованном режиме работы.

Основное окно программы может содержать следующие элементы интерфейса:

1 — Меню
Содержит команды управления программой
2 — Панель инструментов основного окна
Содержит кнопки быстрого вызова команд управления и программных средств
3 — Информационный заголовок
Содержит название выбранной для отображения категории объектов
4 — Панель категорий
Содержит ярлыки для выполнения одноименных команд меню "Вид". Чтобы отобразить в программе объекты, относящиеся к нужной категории, выберите на этой панели ее ярлык
5 — Область списка объектов
Содержит список объектов, связанных с выбранным элементом в окне структуры. По умолчанию для фона строк в списке используется следующее цветовое оформление: • белый фон — объект связан с вышестоящими и нижестоящими объектами; • розовый фон — объект не связан с вышестоящими или нижестоящими объектами; • серый фон — ресурс не поставлен на контроль. В локальном режиме выделяются названия объектов, созданных централизованно. Параметры цветового оформления можно изменить (см. стр.**280**)

6 — Окно структуры
Содержит иерархический список объектов. Корневым элементом иерархии является выбранная категория объектов. Для обозначения объектов используются следующие пиктограммы:  — субъект;  — задание ЗПС;  — тиражируемое задание ЗПС;  — задание КЦ;  — тиражируемое задание КЦ;  — задание ПАК "Соболь";  — задача;  — задача со сценарием;  — группа файлов и каталогов;  — группа сценариев (скриптов);  — группа объектов реестра. Для отображения наличия связей между объектами используются следующие пиктограммы: •  (нижняя половина кружка красная) — объект не включает в себя другие объекты; •  (верхняя половина кружка красная) — объект не включен ни в один из других объектов; • — объект не имеет связей; • ✔ — для объекта установлены все предполагаемые связи с другими объектами. Кнопки панели инструментов этого окна предназначены для управления списком объектов. Окно структуры содержит список объектов той модели данных, которая соответствует разрядности ОС Windows на компьютере. Список объектов доступен для редактирования
7 — Окно структуры модели данных другой разрядности
Присутствует только в централизованном режиме работы программы. По своему назначению окно аналогично окну структуры **(6)**, но содержит список объектов модели данных другой разрядности, чем ОС Windows на компьютере (например, модели для 64-разрядных версий ОС Windows, если на компьютере установлена 32-разрядная ОС). Список объектов отображается в режиме "только для чтения". Можно копировать объекты в окно структуры **(6)** — для этого вызовите контекстное меню нужного объекта и выберите команду "Добавить в рабочую модель..."
8 — Окно зависимостей
Содержит список объектов, связанных с выбранным элементом в области списка объектов. В верхней части окна расположены кнопки, управляющие фильтрацией объектов списка
9 — Строка состояния
Содержит служебные сообщения программы. В правой части строки выделены зоны, в которых помещается следующая информация (по порядку слева направо): • порядковый номер выбранного объекта, общее количество и количество выделенных объектов в области списка объектов или в дополнительном окне зависимостей; • текущее время

Настройка элементов интерфейса

Для удобства работы с программой пользователь может изменять состав отображаемых элементов интерфейса и управлять их размещением в основном окне программы. Внешний вид основного окна сохраняется в системном реестре и используется в следующих сеансах работы пользователя с программой.

Меню и панель инструментов можно перемещать в любое место экрана стандартными способами, принятыми в приложениях ОС Windows.

Панель категорий всегда располагается по левому краю основного окна программы. Положение дополнительных окон зафиксировано и не может быть изменено. Для изменения размеров панели и дополнительных окон используются их внутренние границы.

Управление элементами интерфейса осуществляется командами меню "Вид":

Команда	**Описание**
Вид | Строка состояния	Включает или отключает отображение строки состояния **(9)**
Вид | Панели | Кнопки	Включает или отключает отображение панели инструментов **(2)**

Команда	Описание
Вид | Панели | Заголовок	Включает или отключает отображение информационного заголовка **(3)**
Вид | Панели | Категории	Включает или отключает отображение панели категорий **(4)**
Вид | Панели | Структура	Включает или отключает отображение окна структуры **(6)**
Вид | Панели | Структура на чтение	Включает или отключает отображение окна структуры модели данных другой разрядности **(7)**
Вид | Панели | Зависимости	Включает или отключает отображение окна зависимостей **(8)**

Параметры работы программы

Настройка параметров работы программы осуществляется в диалоге "Настройки приложения". Описание параметров приводится ниже.

Для настройки параметров:

1. Выберите команду "Сервис | Настройки…".

   На экране появится диалог "Настройки приложения".
2. Последовательно выбирая названия групп из списка в левой части диалога, укажите необходимые значения параметров (параметры представлены в правой части). В большинстве случаев для изменения значения параметра выберите нужное значение из раскрывающегося списка.

Группа параметров "Общие | Подтверждения"

Содержит параметры подтверждения выполняемых операций. Если установлено значение "Да", при выполнении данной операции будет выводиться диалог запроса для подтверждения операции.

Группа параметров "Общие | Цвета элементов списка"

Содержит параметры цветового оформления строк таблицы, расположенной в области списка объектов. Ячейка со значением каждого параметра содержит прямоугольник, окрашенный текущим выбранным цветом. Изменение значения параметра осуществляется с использованием стандартных средств выбора цвета, которые вызываются кнопкой в правой части ячейки.

Текст, Фон
Определяют, соответственно, цвета символов и фона для отображения сведений об объектах, которые связаны и с вышестоящими, и с нижестоящими объектами иерархии
Текст ошибки, Фон ошибки
Определяют, соответственно, цвета символов и фона для отображения сведений об объектах, которые не связаны с вышестоящими или нижестоящими объектами
Текст (неконтролируемые), Фон (неконтролируемые)
Определяют, соответственно, цвета символов и фона для отображения: • сведений о ресурсах, для которых не включен признак контроля целостности; • заданий контроля целостности, у которых отсутствует расписание; • заданий ПАК "Соболь" при отсутствии самой платы на компьютере (в локальном режиме работы программы)
Текст (нелокальные), Фон (нелокальные)
Определяют, соответственно, цвета символов и фона для отображения сведений о ресурсах, которые находятся на других компьютерах и являются для данного компьютера сетевыми ресурсами. Используется только в локальном режиме работы программы

Группа параметров "Общие | Интерфейс"

Содержит отдельные параметры интерфейса, не относящиеся к вышеперечисленным группам.

Диалог при подготовке к ЗПС
Если установлено значение "Да", при запуске процедуры подготовки ресурсов для включения их в механизм ЗПС (например, по команде "Сервис | Ресурсы ЗПС") появляется диалог для настройки параметров поиска ресурсов. Если установлено значение "Нет", для подготовки ресурсов будут использованы параметры, заданные в группе параметров "Инструментарий | Подготовка для ЗПС" (см. ниже)
Диалог расчета эталонов
Если установлено значение "Да", при запуске процедуры расчета эталонных значений для контроля целостности (например, по команде "Сервис | Эталоны | Расчет") появляется диалог для настройки параметров расчета. Если установлено значение "Нет", для расчета эталонных значений используются параметры, заданные в группе параметров "Инструментарий | Расчет эталонов" (см. ниже)
Сетка в списке
Если установлено значение "Да", в области списка объектов и в дополнительном окне зависимостей отображаются линии, разделяющие ячейки таблиц

Группа параметров "Инструментарий | Подготовка для ЗПС"

Содержит параметры, задаваемые по умолчанию при подготовке списка ресурсов для включения их в механизм замкнутой программной среды.

Перевыбор выполняемых
Если установлено значение "Да", перед поиском выполняемых ресурсов (файлов) программа автоматически сбрасывает признак "выполняемый" со всех ресурсов, имеющихся в модели данных. Это позволяет установить признак "выполняемый" только для тех ресурсов, которые удовлетворяют заданным параметрам поиска. Если установлено значение "Нет", сброс признака не осуществляется
Расширения выполняемых
Содержит список расширений файлов. Список применяется при поиске выполняемых ресурсов или добавлении новых ресурсов (кроме единичных файлов). Признаки "выполняемый" будут установлены для тех файлов, расширения которых входят в этот список. Изменение значения параметра осуществляется редактированием текстового содержимого поля. Список расширений оформляется следующим образом: .<*расширение1*>; <…>; .<*расширениеN*> При централизованном управлении список действует на компьютерах с версией ОС соответствующей разрядности (32- или 64-разрядные версии) и относящихся к субъектам, для которых в параметрах механизма ЗПС действует параметр "Режимы заданы централизованно"
Имена исполняемых модулей процессов
Содержит список имен файлов, которые являются исполняемыми модулями процессов, но расширения в именах отличаются от стандартного .exe (например, soffice.bin, someimage.imgext). Для указанных файлов будут доступны такие же функции настройки и контроля, как и для файлов с расширением .exe
Добавлять модули
Если установлено значение "Да", при поиске выполняемых ресурсов программа включает в список ресурсов "зависимые модули" (файлы, от которых зависит выполнение исходных файлов, например, все библиотеки, необходимые для запуска winword.exe). При отсутствии в модели данных описания зависимого модуля оно будет автоматически создано и добавлено в группу ресурсов, содержащую описание исходного файла. Включение зависимых модулей осуществляется рекурсивно — файлы, от которых зависит выполнение самих зависимых модулей, также включаются в список. Если установлено значение "Нет", поиск зависимых модулей не осуществляется

Группа параметров "Инструментарий | Расчет эталонов"

Содержит значения по умолчанию для параметров процедуры расчета эталонных значений.

Оставлять старые
Если установлено значение "Да", рассчитанные ранее эталонные значения будут сохранены в списке эталонных значений ресурса после очередной процедуры расчета. Если установлено значение "Нет", все рассчитанные ранее эталоны удаляются
Не поддерживается
Определяет реакцию программы в случае, если определенный в задании метод или алгоритм контроля целостности неприменим к ресурсу: • "Игнорировать" — никакие действия не предпринимаются; • "Выводить запрос" — на экран выводится диалог для выбора варианта продолжения процедуры; • "Удалять ресурс" — ресурс удаляется из общего списка ресурсов (из модели данных); • "Ресурс снимать с контроля" — для ресурса сбрасывается признак "контролировать"
Нет доступа
Определяет реакцию программы в случае, если при попытке расчета эталонного значения программа не получила доступ к ресурсу (например, отсутствует доступ на чтение файла или файл заблокирован другим процессом). Выбор вида реакции осуществляется так же, как для параметра "Не поддерживается"
Ресурс отсутствует
Определяет реакцию программы в случае, если при попытке расчета эталонного значения программа не обнаружила ресурс (например, файл был перемещен). Выбор вида реакции осуществляется так же, как для параметра "Не поддерживается"

Группа параметров "Инструментарий | Импорт и добавление"

Содержит значения по умолчанию для параметров процедур импорта объектов и добавления ресурсов в модель данных.

С учетом существующих
Если установлено значение "Да", то при импорте объектов, одноименных объектам текущей модели данных, они замещают объекты модели. Если установлено значение "Нет", то объекты модели остаются неизменными, а импортируемые объекты переименовываются следующим образом: *имя_объекта*<*N*>, где *N* — порядковый номер дублируемого объекта (например, "Группа ресурсов" и "Группа ресурсов1")
Помечать выполняемые
Если установлено значение "Да", то при добавлении новых файлов в модель данных (кроме добавления единичных файлов) автоматически присваивается признак "выполняемый" для тех файлов, расширения которых входят в список "Расширения выполняемых", или указанных в списке "Имена исполняемых модулей процессов". Если установлено значение "Нет", такая проверка не выполняется

Группа параметров "Оповещения | Общие"

Содержит единственный параметр рассылки оповещений об изменениях в модели данных. Используется только в режиме централизованного управления.

Рассылка при сохранении
Если установлено значение "Да", при сохранении модели данных на все компьютеры домена безопасности, в отношении которых модель данных изменилась, будет отправлено оповещение об изменениях

Группа параметров "Хранилище объектов | Удаленные объекты"

Содержит единственный параметр настройки удаления объектов из централизованной модели данных. Используется только в режиме централизованного управления.

Время жизни
Определяет время, в течение которого объект централизованной модели данных, помеченный для удаления, остается в хранилище объектов централизованного управления и учитывается при синхронизации. Значение параметра задается в часах

Средства для работы со списками объектов

Навигация при работе со структурами объектов

Переходы между элементами структуры в некоторых случаях удобно выполнять с помощью стандартных команд навигации и кнопок панели инструментов.

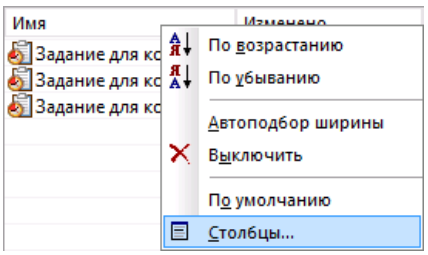
Команда	Кнопка	Описание
Вид | Назад		Выполняет переход к предыдущему выбранному элементу структуры
Вид | Вперед		Выполняет переход к следующему выбранному элементу структуры
Вид | Домой		Выполняет переход к корневому элементу структуры

Настройка отображения колонок в таблицах

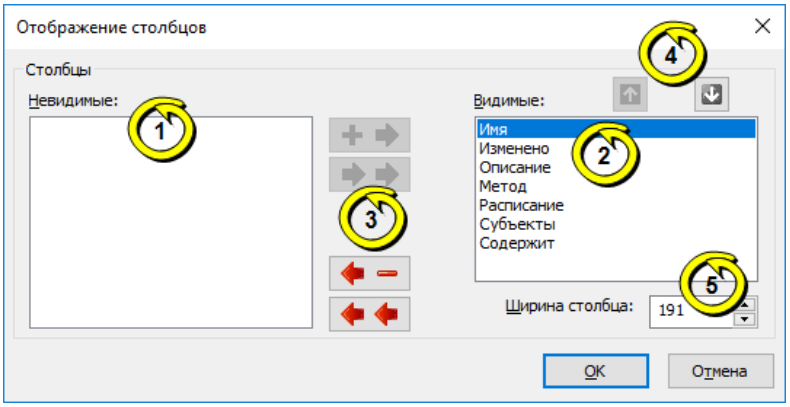
В области списка объектов и в окне зависимостей используется табличная форма представления списков объектов. Состав колонок таблицы зависит от того, объекты какой категории отображаются. Для оптимального отображения информации можно изменять ширину колонок, добавлять или удалять колонки либо перемещать колонки относительно других. Эти действия аналогичны стандартным операциям в ОС Windows.

Для управления колонками с помощью диалога настройки:

1. Вызовите контекстное меню в строке заголовков колонок и выберите команду "Столбцы...".



На экране появится диалог настройки параметров отображения колонок.



Пояснение. На рисунке обозначены: 1 — список колонок, не отображаемых в таблице; 2 — список отображаемых колонок; 3 — кнопки перемещения из списка в список; 4 — кнопки формирования порядка следования колонок; 5 — поле ввода ширины выбранной колонки (в пикселях).

2. Настройте параметры отображения колонок.

Для восстановления исходного состояния таблицы:

- Вызовите контекстное меню заголовка колонки и выберите команду "По умолчанию".

Внешний вид таблицы (ширина и состав колонок) будет восстановлен в соответствии с исходными настройками программы.

Сортировка списков объектов

Таблицы в области списка объектов и окна зависимостей сортируются по значениям, содержащимся в определенных колонках. Способы сортировки аналогичны стандартным способам управления таблицами, принятым в большинстве приложений Windows. В заголовке колонки, по которой отсортирована таблица, указывается соответствующее направление сортировки.

Поиск объектов в списках

Поиск осуществляется по значениям, содержащимся в отображаемых колонках таблицы из области списка объектов или дополнительного окна зависимостей.

Для поиска объекта:

1. Выберите в таблице объект, с которого начнется поиск.
2. Выберите команду "Правка | Найти...".

   На экране появится диалог настройки параметров поиска.
3. В поле "Что" введите строку поиска и при необходимости настройте параметры поиска. Нажмите кнопку "ОК".

Учитывать регистр
Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых содержится заданная строка символов в том же регистре. При отсутствии отметки регистр символов не учитывается
Целиком значение
Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых заданная строка символов содержится в виде отдельного слова (слов). При отсутствии отметки строка символов может являться частью других строк
Искать в поле
При наличии установленной отметки параметр определяет имя колонки (в раскрывающемся списке справа), по которой будет выполняться поиск в таблице. Если отметка отсутствует, поиск осуществляется во всех отображаемых колонках в таблице

Программа выполнит поиск и выделит найденный объект в таблице. Если искомая строка не найдена, на экране появится соответствующее сообщение.

Чтобы найти другие объекты, удовлетворяющие заданным параметрам поиска, процедуру поиска можно продолжить, начиная с текущего выбранного объекта.

Переходы по связям объектов

При правильной организации модели данных каждый объект должен входить в одну или несколько цепочек связанных между собой ("зависимых") объектов. Если требуется определить, с какими объектами связан данный объект, используется окно зависимостей (см. стр.**279**).

Для перехода к связанному объекту:

1. В области списка объектов выберите объект или группу объектов.

   В окне зависимостей появится список объектов.
2. При необходимости настройте в окне зависимостей фильтрацию по категориям представления объектов. Для переключения режима фильтрации могут использоваться ярлыки в верхней части окна зависимостей.
3. В списке объектов окна зависимостей найдите объект, к которому требуется перейти в структуре объектов, вызовите контекстное меню объекта и выберите команду "Перейти в дереве".

В окне структуры будет раскрыта соответствующая ветвь дерева и выделен искомый объект.

Резервное копирование БД КЦ-ЗПС с использованием командной строки

Экспорт и импорт модели данных КЦ-ЗПС можно выполнять путем запуска программы "Контроль программ и данных" из командной строки. Для запуска необходимо перейти в каталог установки клиента и запустить на исполнение файл SnICheckAdm.exe с нужными параметрами.

Перечень предусмотренных параметров представлен в таблице.

Параметр	Значение	Описание
HIDE	Отсутствует	Блокирует открытие окна программы
MODE	LOCAL CENTRAL	Локальный режим работы (по умолчанию). Централизованный режим работы
LOAD	Отсутствует	Выполняется загрузка модели данных из БД (ЛБД или ЦБД — зависит от режима работы)
IMPORT	Имя файла в кавычках, например: "C:\Catalog 1\model.xml"	Импорт модели данных из файла
EXPORT	Имя файла в кавычках, например: "C:\Catalog 1\model.xml"	Экспорт модели данных в файл
SAVE	Отсутствует	Выполняется сохранение модели данных в БД (ЛБД или ЦБД — зависит от режима работы)
CALC	Отсутствует	Выполняется расчет эталонов. Модель данных предварительно должна быть сохранена. Реакция на ошибки во время расчета — в соответствии с параметрами, заданными в программе
EXIT	FORCE (необязательно)	Завершает работу программы. Если присутствует значение Force, не выполняется проверка сохранения изменений в БД (и не выводится соответствующий запрос при наличии несохраненных изменений)

Заданные параметры применяются в порядке их следования в командной строке (слева направо). Регистр символов не учитывается.

Перед каждым параметром необходимо добавлять символ "/" или "-". Все элементы строки (параметры, значения) разделяются пробелами.

Пример использования:

SnICheckAdm.exe /hide /mode central /load /export "D:\Dir1\Data.xml" /exit force

В приведенном примере выполняется запуск программы в централизованном режиме работы без открытия окна. В программу загружается модель данных из ЦБД и затем экспортируется в указанный XML- файл. После экспорта завершается работа программы без проверки несохраненных изменений.

Общие сведения о программе настройки для режима контроля потоков

Программа настройки для режима контроля потоков предназначена для настройки параметров, обеспечивающих функционирование механизма полномочного управления доступом в режиме контроля потоков. Сведения о запуске программы и условиях работы с ней см. на стр.**167**.

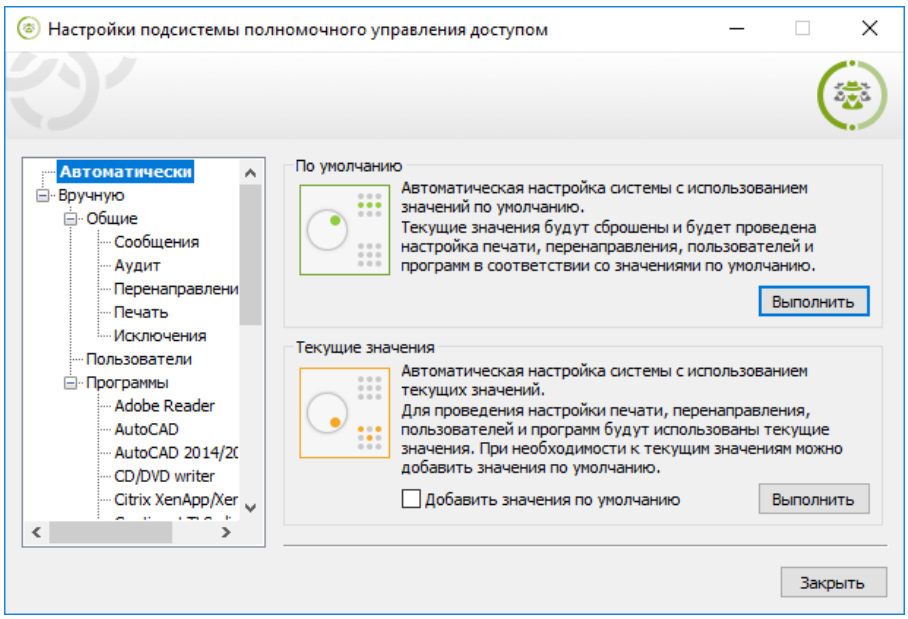
Автоматическая настройка

Настройка системы для функционирования механизма полномочного управления доступом и контроля печати может выполняться автоматически. Для автоматической настройки предусмотрены возможности использования значений параметров, задаваемых по умолчанию, или текущих заданных значений, сконфигурированных при настройке вручную.

Автоматическая настройка со значениями по умолчанию применяется в случае необходимости удалить текущую конфигурацию и вернуть исходные значения параметров. Это может потребоваться, если значения параметров некорректно заданы или удалены, а также при первичной настройке системы с минимально необходимой конфигурацией для функционирования механизма в режиме контроля потоков.

Настройка с текущими значениями предназначена для повторного применения в системе заданных значений параметров. Это позволяет восстановить настройку системы при сбоях функционирования механизма или при добавлении в систему новых пользователей, программ, принтеров и других объектов, задействованных в механизме полномочного управления доступом и контроля печати. При такой настройке дополнительно к текущим значениям параметров можно добавить исходные значения (значения по умолчанию). При этом текущие значения не удаляются.

Чтобы выполнить автоматическую настройку, в левой панели окна программы выберите режим "Автоматически".



Для удаления текущей конфигурации и настройки системы со значениями по умолчанию:

- В разделе "По умолчанию" нажмите кнопку "Выполнить".

  Начнется процесс автоматической настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Для настройки системы с текущими значениями параметров:

1. Если к текущим значениям параметров требуется добавить исходные значения, установите отметку в поле "Добавить значения по умолчанию".
2. В разделе "Текущие значения" нажмите кнопку "Выполнить".

   Начнется процесс автоматической настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Настройка вручную

Программа настройки предоставляет возможность вручную изменять параметры, относящиеся к работе механизма полномочного управления доступом и контроля печати. Это позволяет обеспечить функционирование механизма с учетом особенностей программной среды компьютера и предпочтений пользователя.

Средства для ручной настройки параметров представлены в следующих основных разделах:

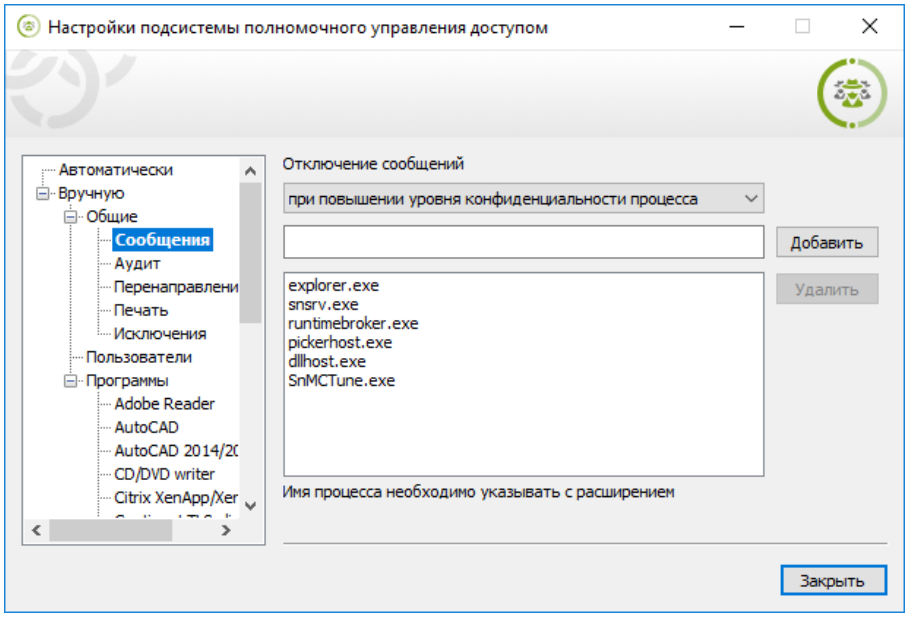
- "Общие" — для настройки общих параметров работы пользователей и приложений;
- "Пользователи" — для настройки параметров, относящихся к профилям пользователей;
- "Программы" — для настройки параметров, относящихся к приложениям.

Отключение вывода предупреждающих сообщений системы

В определенных случаях система выводит пользователю предупреждающие сообщения об изменении категорий конфиденциальности файлов или процессов. Для удобной работы пользователя предусмотрены возможности отключения вывода сообщений в следующих случаях:

- при повышении уровня конфиденциальности процесса (например, explorer.exe) по причине доступа к файлу с более высокой категорией конфиденциальности (применимо при отключенном режиме контроля потоков);
- при повышении категории конфиденциальности файла, имеющего указанное расширение, или файла из указанного каталога. Данная возможность предназначена для обеспечения автоматического создания и редактирования служебных файлов, используемых некоторыми приложениями (например, редактором MS Word), в режиме контроля потоков при работе в конфиденциальных сессиях;
- при выводе конфиденциального файла, имеющего указанное расширение, на внешние носители, в результате чего происходит сброс категории конфиденциальности отчуждаемого файла (применимо в режиме контроля потоков при работе в конфиденциальных сессиях).

Чтобы настроить параметры отключения вывода сообщений, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Сообщения".



Для отключения сообщений при повышении уровня конфиденциальности процессов:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня конфиденциальности процесса".

   Ниже будет выведен список процессов (имена исполняемых файлов), для которых вывод сообщений данного типа отключен.
2. Отредактируйте список имен файлов:
   - чтобы добавить элемент в список, введите в строке имя исполняемого файла процесса (с указанием расширения) и нажмите кнопку "Добавить";
   - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".

Для отключения сообщений при повышении категории конфиденциальности файлов с определенными расширениями:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня файла (по расширению)".

   Ниже будет выведен список расширений файлов, для которых вывод сообщений данного типа отключен.
2. Отредактируйте список расширений:
   - чтобы добавить элемент в список, введите в строке расширение имени файла в виде .<расширение> (например, .lnk) и нажмите кнопку "Добавить";
   - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить";
   - чтобы отключить вывод сообщений для файлов с любыми расширениями, добавьте в список элемент .* или установите отметку в поле "Отключить вывод сообщений для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Для отключения сообщений при повышении категории конфиденциальности файлов из определенных каталогов:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня файла (для директории)".

   Ниже будет выведен список каталогов, для файлов которых вывод сообщений данного типа отключен (независимо от расширений файлов).

2. Отредактируйте список путей к каталогам:
   - чтобы добавить элемент в список, введите в строке путь к каталогу и нажмите кнопку "Добавить";

     Примечание. Ввод пути к каталогу выполняется с учетом следующих особенностей:
     - строка может содержать как полный путь, однозначно определяющий данный каталог, так и часть пути, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
     - путь к каталогу указывается БЕЗ символа "\" на конце;
     - имена каталогов должны быть указаны в формате LFN.

   - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".

Для отключения сообщений при выводе конфиденциальной информации на внешние носители:

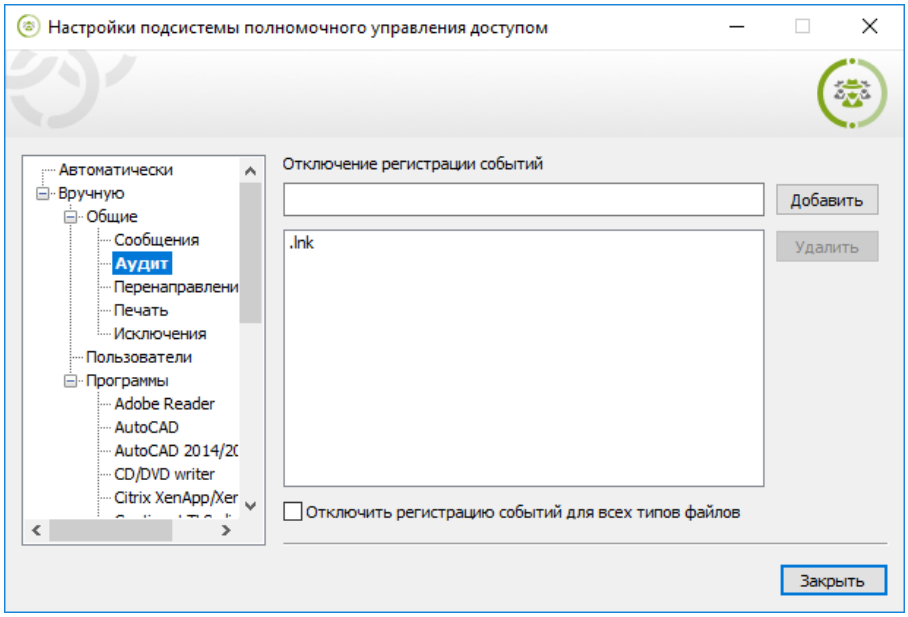
1. В поле "Отключение сообщений" укажите значение "при выводе конфиденциальной информации (по расширению)".

   Ниже будет выведен список расширений файлов, для которых вывод сообщений данного типа отключен.
2. Отредактируйте список расширений:
   - чтобы добавить элемент в список, введите в строке расширение имени файла в виде .<расширение> (например, .lnk) и нажмите кнопку "Добавить";
   - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить";
   - чтобы отключить вывод сообщений для файлов с любыми расширениями, добавьте в список элемент .* или установите отметку в поле "Отключить вывод сообщений для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Отключение регистрации событий обращения к файлам

В журнале Secret Net Studio осуществляется регистрация событий внутрисистемных обращений к файлам при функционировании механизма полномочного управления доступом и контроля печати. При необходимости регистрацию таких событий можно отключить применительно к файлам, имеющим определенные расширения. Это позволяет сократить объем информации, сохраняемой в журнале.

Чтобы настроить параметры отключения регистрации событий, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Аудит".



Для отключения регистрации событий обращения к файлам с определенными расширениями:

- Сформируйте список расширений файлов:
  - чтобы добавить элемент в список, введите в строке расширение имени файла в виде .<расширение> (например, .lnk) и нажмите кнопку "Добавить";
  - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить";
  - чтобы отключить регистрацию событий для файлов с любыми расширениями, добавьте в список элемент .* или установите отметку в поле "Отключить регистрацию событий для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Перенаправление вывода общих служебных файлов

Механизм полномочного управления доступом и контроля печати выполняет проверку соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталог, файл). Однако в ряде приложений (например MS Word) происходят обращения к служебным файлам, которые хранятся в специальных каталогах. При этом отсутствуют возможности изменять категории конфиденциальности этих файлов в зависимости от уровня допуска пользователя. При использовании механизма полномочного управления доступом в режиме контроля потоков такие особенности приводят к конфликтным ситуациям и невозможности корректной работы приложений.

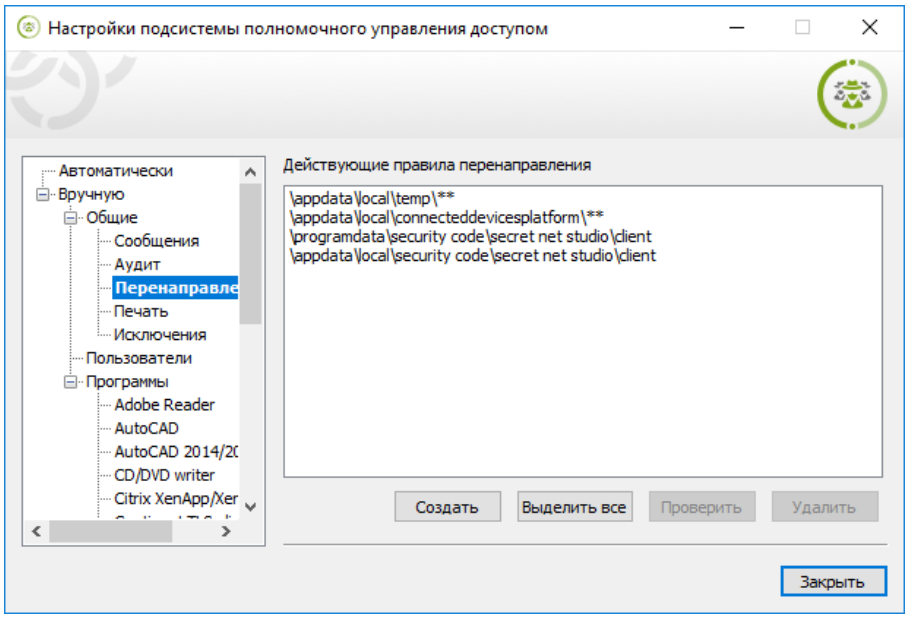
Для устранения этой проблемы в системе реализована функция перенаправления вывода общих служебных файлов. Функция действует при работе в конфиденциальных сессиях. Чтобы обеспечить работу приложения в сессиях с различными уровнями конфиденциальности, создаются отдельные каталоги (по количеству категорий), в которых служебным файлам назначаются соответствующие категории конфиденциальности. Если приложение в конфиденциальной сессии осуществляет попытку обращения к общему файлу, система перенаправляет это обращение к копии общего файла, находящейся в отдельном каталоге, который был создан для сессий данного уровня конфиденциальности.

При настройке параметров перенаправления вывода файлов формируется список путей к каталогам с общими файлами, для которых должны быть созданы дополнительные каталоги с различными категориями конфиденциальности. В этих каталогах будут храниться файлы, используемые в сессиях соответствующих уровней конфиденциальности. Например, для обслуживания обращений приложения MS Word русской версии в списке должна присутствовать запись \AppData\Roaming\Microsoft\Шаблоны. В зависимости от уровня конфиденциальности сессии пользователя при обращении приложения к данным каталогам чтение/запись информации для общих файлов будет выполняться в одном из дополнительно созданных подкаталогов \Шаблоны(1), \Шаблоны(2) и т. д. в каталоге \AppData\Roaming\Microsoft.

Примечание. Следствием действия функции перенаправления вывода является независимость сделанных изменений в общих служебных файлах при работе с приложением в сессиях с различными уровнями конфиденциальности. Например, если общий файл был изменен в сессии с уровнем "строго конфиденциально", эти изменения не будут учтены в сессиях с другими уровнями конфиденциальности, так как в этих сессиях обращение осуществляется к другим копиям общего файла.

При автоматической настройке системы (см. стр.**287**) создание каталогов перенаправления выполняется только для системного диска. Если список путей формируется вручную, предоставляется возможность выбора дисков.

Чтобы сформировать список путей для перенаправления вывода файлов, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Перенаправление".



Для добавления путей в список:

1. Нажмите кнопку "Создать".

   На экране появится диалог для добавления путей к каталогам.

2. Сформируйте в диалоге список добавляемых путей:

   - чтобы добавить элемент в список, введите в строке путь к каталогу и нажмите кнопку "Добавить";

Примечание. Ввод пути к каталогу выполняется в формате LFN с учетом следующих особенностей:

- строка может содержать как полный путь, однозначно определяющий данный каталог, так и часть пути, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
- путь к каталогу указывается БЕЗ символа "\" на конце;
- если в каталоги перенаправления не требуется копировать файлы из исходного каталога — добавьте в конце пути шаблонную подстроку "**" (с двумя символами "звездочка"). В этом случае в каталогах перенаправления будет создана структура подкаталогов исходного каталога без файлов. Например, данный вариант применяется по умолчанию для каталогов временных файлов пользователей;
- если в каталоги перенаправления не требуется копировать подкаталоги исходного каталога — добавьте в конце пути шаблонную подстроку "*" (с одним символом "звездочка"). В этом случае в каталогах перенаправления будут созданы только копии файлов исходного каталога.

- чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".

3. Нажмите кнопку "Создать".
4. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов. В диалоге отметьте нужные диски и нажмите кнопку "ОК".

   Начнется процесс поиска каталогов, удовлетворяющих добавляемым путям. Для найденных каталогов будут созданы каталоги <*имя_ каталога*> (1), <*имя_ каталога*> (2) и т. д. с соответствующими категориями конфиденциальности (например, "конфиденциально" для первого каталога и "строго конфиденциально" для второго). В созданные каталоги будет скопировано содержимое исходных каталогов (в зависимости от указанных шаблонных подстрок). По окончании процесса поиска пути к каталогам будут добавлены в список путей для перенаправления вывода файлов.

Примечание. Возможность выбора дисков позволяет ускорить процесс поиска каталогов за счет пропуска содержимого неотмеченных дисков. Однако из-за этого могут возникнуть ситуации, когда заданным путям будут удовлетворять каталоги на необработанных дисках. В таких случаях система будет выполнять попытки перенаправления вывода для этих каталогов, но из-за отсутствия на диске соответствующих структур приложение может функционировать некорректно. Поэтому если поиск каталогов осуществляется не на всех дисках, рекомендуется указывать такие пути, для которых отсутствуют соответствующие каталоги на неотмеченных дисках.

Для проверки возможности перенаправления:

1. Выделите в списке пути, для которых требуется проверить действие функции перенаправления (для выделения всех элементов списка нажмите кнопку "Выделить все").
2. Нажмите кнопку "Проверить".
3. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов. В диалоге отметьте нужные диски и нажмите кнопку "ОК".

   Начнется процесс поиска каталогов, удовлетворяющих выбранным путям. Для найденных каталогов будет проверено наличие и корректность настройки каталогов <*имя_ каталога*> (1), <*имя_ каталога*> (2) и т. д. с соответствующими категориями конфиденциальности. При необходимости каталоги будут созданы и заполнены заново. По окончании процесса поиска и проверки на экране появится соответствующее сообщение.

Для удаления путей из списка:

1. Выделите в списке пути, которые требуется удалить (для выделения всех элементов списка нажмите кнопку "Выделить все").
2. Нажмите кнопку "Удалить".

   Выбранные пути будут незамедлительно удалены из списка. При этом сами каталоги перенаправления и содержащиеся в них файлы удалены не будут.

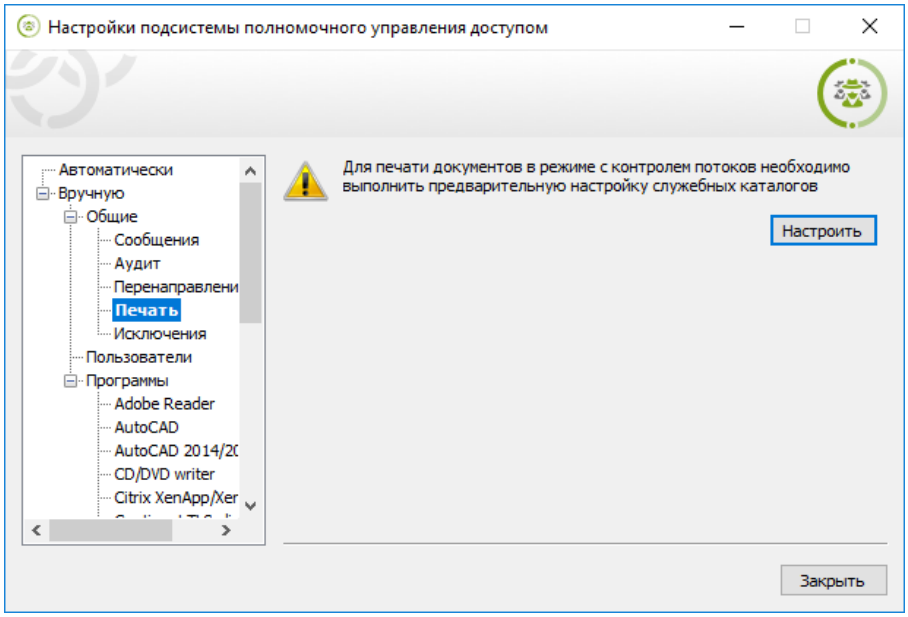
Настройка системы для печати на принтер

Для печати на принтер в режиме контроля потоков (при работе в конфиденциальных сессиях) должна быть выполнена настройка некоторых служебных каталогов ОС Windows.

Настройка параметров каталогов в необходимом объеме осуществляется при общей автоматической настройке (см. стр.**287**).

Программа настройки осуществляет проверку текущих заданных параметров в системе. Если обеспечивается возможность печати на принтер в режиме контроля потоков, средства для настройки печати неактивны. При выявлении необходимости проведения настройки программа предоставляет возможность запустить процесс вручную.

Чтобы настроить систему для печати на принтер, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Печать".



Для запуска процесса настройки печати:

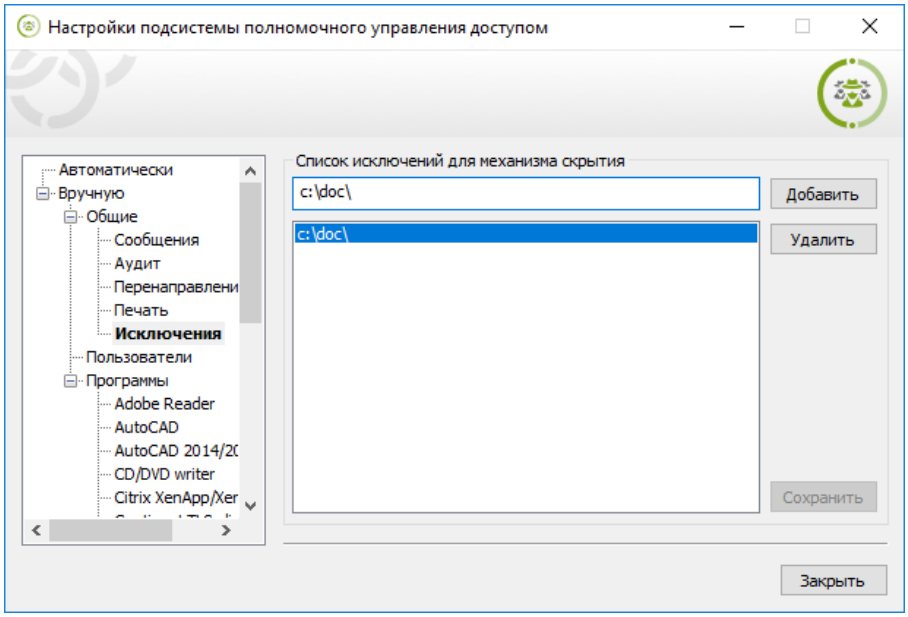
- Нажмите кнопку "Настроить" (кнопка активна, если настройка не проведена в нужном объеме).

  Начнется процесс настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Настройка списка исключений для режима скрытия файлов

Для механизма скрытия конфиденциальных файлов можно составить список файлов и каталогов, на которые не будут действовать правила скрытия.

Чтобы настроить список исключений, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Исключения".



Для настройки списка исключений:

1. Сформируйте список путей к каталогам и файлам:
   - чтобы добавить элемент в список, введите в строке нужный путь и нажмите кнопку "Добавить";

     Пояснение. При вводе пути учитывайте следующие правила:
     - строка может содержать как полный путь, однозначно определяющий ресурс, так и часть пути, задающую подмножество путей к ресурсу. Если указывается подмножество путей, строка должна начинаться символом "\";
     - путь к каталогу должен всегда оканчиваться символом "\", C:\doc воспринимается программой как путь к файлу;
     - символы "*" в конце строки указывают, что в список исключений добавляются как файлы из данного каталога, так и файлы из всех подкаталогов всех уровней вложенности (например, C:\doc*).
   - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".
2. Завершив формирование списка, нажмите кнопку "Сохранить" для сохранения и применения списка исключений.

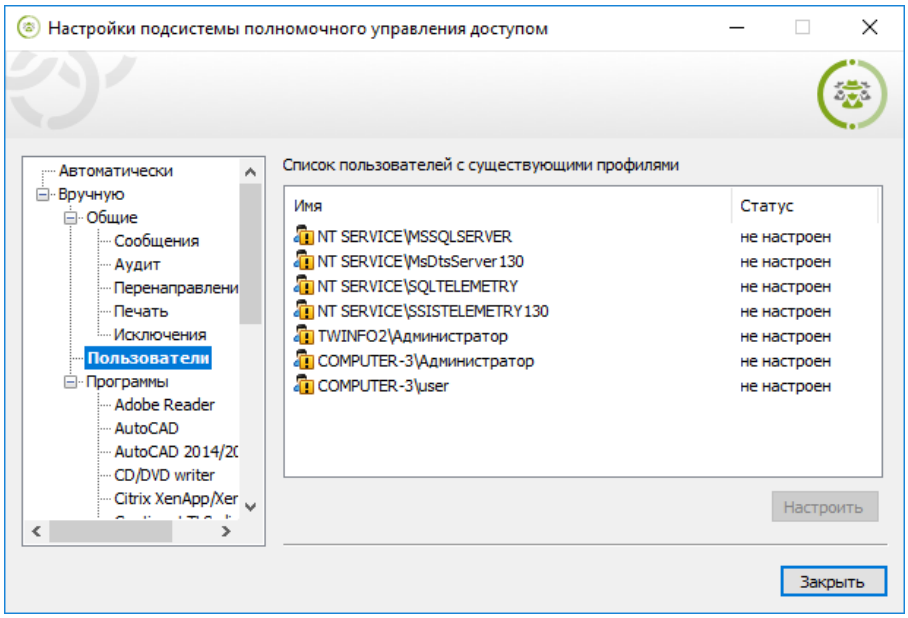
Настройка параметров, относящихся к профилям пользователей

Для работы пользователя в режиме контроля потоков (в конфиденциальных сессиях) должна быть выполнена настройка параметров, относящихся к профилю этого пользователя. Настройка заключается в создании структуры каталогов перенаправления вывода файлов для временных каталогов пользователя и установке соответствующих категорий конфиденциальности с определенной конфигурацией признаков наследования для этих каталогов. Настройка выполняется для тех пользователей, от имени которых хотя бы раз был выполнен вход в систему на данном компьютере.

Настройка всех профилей пользователей в необходимом объеме осуществляется при общей автоматической настройке (см. стр.**287**). При добавлении в систему нового пользователя или при переименовании существующего необходимо выполнить настройку профиля этого пользователя для работы в режиме контроля потоков. Запуск процесса настройки профилей можно выполнить вручную.

Программа настройки осуществляет проверку текущих заданных параметров профилей пользователей. Если обеспечивается возможность работы пользователя в режиме контроля потоков, для этого пользователя отображается статус "настроен". При выявлении необходимости проведения настройки для пользователя отображается статус "не настроен".

Чтобы настроить профили пользователей, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Пользователи".



Для запуска процесса настройки профилей пользователей:

1. Выделите в списке пользователей, профили которых необходимо настроить (если для профиля пользователя настройка уже выполнена, он имеет статус "настроен").
2. Нажмите кнопку "Настроить".

   Начнется процесс настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Формирование списка приложений, подлежащих настройке

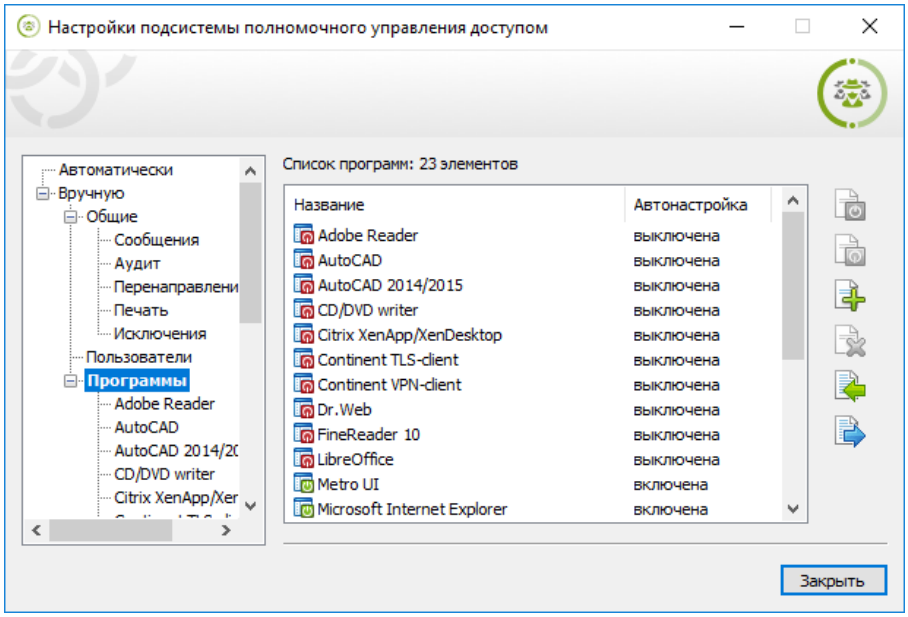
Некоторые приложения не полностью совместимы с механизмом полномочного управления доступом в режиме контроля потоков. Для корректного функционирования таких приложений требуется дополнительная настройка параметров, относящихся к приложению.

С помощью программы может осуществляться настройка параметров для приложений, представленных в списке. Список формируется независимо от наличия на компьютере установленных приложений. По умолчанию после установки клиентского ПО системы защиты список содержит названия программ, для которых выявлена несовместимость и определены необходимые действия по настройке на момент выпуска данной версии системы Secret Net Studio.

Настройка параметров, относящихся к приложениям, может осуществляться при общей автоматической настройке (см. стр. **287**). Автоматическая настройка со значениями по умолчанию всегда применяется к тем приложениям, для которых установлен статус автоматической настройки "включена" в сформированном по умолчанию списке приложений (например, для приложения Microsoft Office). При этом наличие приложения в текущем списке и его статус автоматической настройки не учитываются. Если выполняется автоматическая настройка с текущими значениями, она применяется только к тем приложениям, которые имеют статус "включена" в текущем списке приложений.

Запуск процесса настройки параметров приложения можно также выполнить и вручную.

Чтобы сформировать список приложений, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Программы".



При формировании списка приложений можно выполнять следующие операции:

- импорт списка из xml-файла (с предварительным удалением всех элементов текущего списка);
- экспорт текущего списка в xml-файл;
- управление режимом автоматической настройки приложений;
- добавление списка из xml-файла (без удаления элементов текущего списка);
- удаление выбранных элементов списка.

Для импорта списка из xml-файла:

1. Нажмите кнопку "Импортировать список программ".

   На экране появится стандартный диалог выбора файла.
2. Выберите нужный файл.

   В программу будет загружен список приложений, хранящийся в указанном файле. При этом текущий список будет удален.

Для экспорта списка в xml-файл:

1. Нажмите кнопку "Экспортировать список программ".

   На экране появится стандартный диалог сохранения файла.
2. Укажите имя и место расположения сохраняемого файла.

Для управления режимом автоматической настройки приложений:

1. Выделите в списке приложения, для которых требуется включить или отключить режим автоматической настройки.
2. Нажмите соответствующую кнопку:
   - чтобы включить режим, нажмите кнопку "Включить автоматическую настройку";
   - чтобы отключить режим, нажмите кнопку "Выключить автоматическую настройку".

   Будет установлен соответствующий статус автоматической настройки выбранных приложений.

Для добавления списка из xml-файла:

1. Нажмите кнопку "Добавить программы".

   На экране появится стандартный диалог выбора файла.
2. Выберите нужный файл.

В дополнение к текущему списку приложений в программу будет загружен список, хранящийся в указанном файле.

Для удаления приложений из списка:

1. Выделите в списке приложения, которые требуется удалить.
2. Нажмите кнопку "Удалить программы" и подтвердите решение в появившемся диалоге запроса.

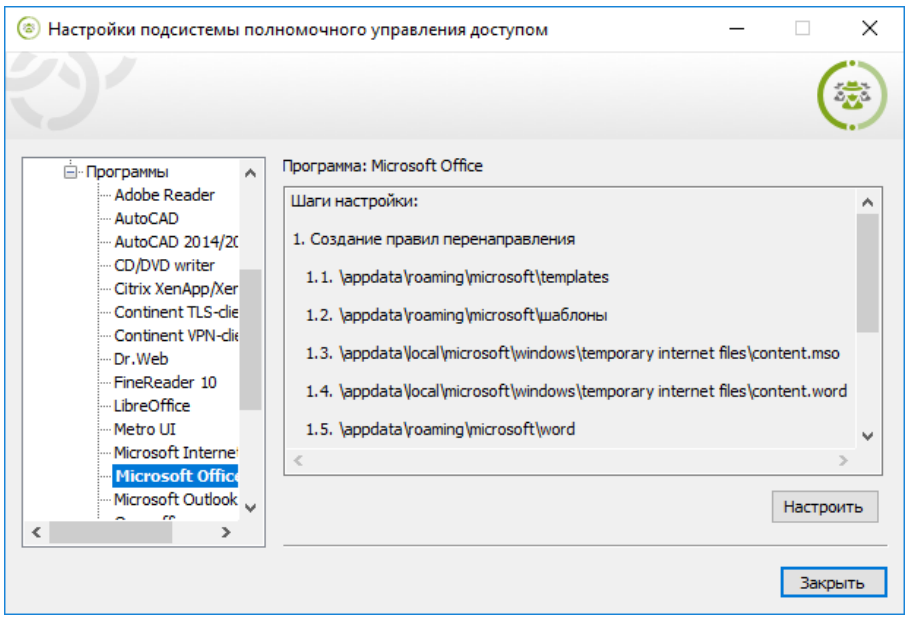
   Выбранные приложения будут незамедлительно удалены из списка.

Настройка параметров приложения

Для корректного функционирования приложения в режиме контроля потоков (при работе в конфиденциальных сессиях) должна быть выполнена настройка параметров, относящихся к этому приложению. Сведения о том, какие действия выполняются программой при настройке, приведены в виде последовательности шагов.

Настройка параметров, относящихся к приложению, может осуществляться автоматически, если в списке приложений установлен статус автоматической настройки "включена". Также запуск процесса настройки для данного приложения можно выполнить вручную.

Чтобы настроить параметры, относящиеся к приложению, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Программы | <имя_приложения>".



Для запуска процесса настройки параметров приложения:

1. Нажмите кнопку "Настроить".
2. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов для создания правил перенаправления. В диалоге отметьте нужные диски и нажмите кнопку "OK".

   Начнется процесс настройки параметров. По окончании процесса на экране появится соответствующее сообщение.

Аварийное снятие защиты локальных дисков

Для отключения режима защиты логических разделов предусмотрены штатные процедуры (см. стр.**180**). В тех случаях, когда такие процедуры по каким-либо причинам не могут быть выполнены, можно использовать загрузочный диск аварийного восстановления.

Использование загрузочного диска аварийного восстановления

Загрузочный диск аварийного восстановления используется при невозможности загрузки ОС штатным способом с системного диска. Например, если происходит сбой при раскодировании модифицированных данных системного диска, что приводит к блокировке загрузки.

С помощью загрузочного диска можно восстановить первоначальное состояние загрузочной области на физическом диске, с которого осуществляется загрузка ОС, и/или загрузочных секторов логических разделов. Процедура создания диска аварийного восстановления описана на стр.**178**.

Внимание! Для загрузки с диска аварийного восстановления на компьютере должна быть включена функция загрузки с внешних носителей. Например, для загрузки с USB-флеш-накопителя может потребоваться включение режима эмуляции Floppy или Forced FDD в BIOS компьютера.

При загрузке с диска аварийного восстановления автоматически запускается программа, которая проверяет возможность восстановления дисков. Если найдены модифицированные диски, которые можно восстановить с помощью ключа на загрузочном диске, на экране появляются запросы на снятие защиты с логических разделов и восстановление соответствующих областей системного диска. Чтобы вернуть первоначальное состояние объекта, нажмите в диалоге запроса кнопку "Да".

Диск аварийного восстановления для механизмов защиты диска и полнодискового шифрования

Диск аварийного восстановления предоставляет следующие возможности:

- смена пароля доступа к зашифрованным дискам (см. стр.**301**);
- сброс пароля доступа к зашифрованным дискам с помощью кода восстановления (см. стр.**302**);
- расшифрование данных на зашифрованных дисках и снятие защиты диска (см. стр.**302**);
- восстановление или удаление загрузчика Secret Net Studio (см. стр.**303**);
- восстановление файла конфигурации подсистем защиты диска и полнодискового шифрования (см. стр.**304**);

  Пояснение. Файл конфигурации подсистем защиты диска и полнодискового шифрования содержит всю информацию о зашифрованных / защищенных дисках компьютера.
- удаление файла конфигурации подсистем защиты диска и полнодискового шифрования (см. стр.**305**);
- удаление зашифрованного диска из конфигурации подсистемы полнодискового шифрования (см. стр.**305**).

Для работы с диском аварийного восстановления необходимо выполнить загрузку с этого диска. Операции выполняются в консольном режиме с помощью клавиатуры.

Пояснение. В данном разделе приведены снимки экрана интерфейса диска аварийного восстановления для UEFI-систем. Интерфейс диска для MBR-систем отличается.

Рис.7 Главное меню диска аварийного восстановления Secret Net Studio

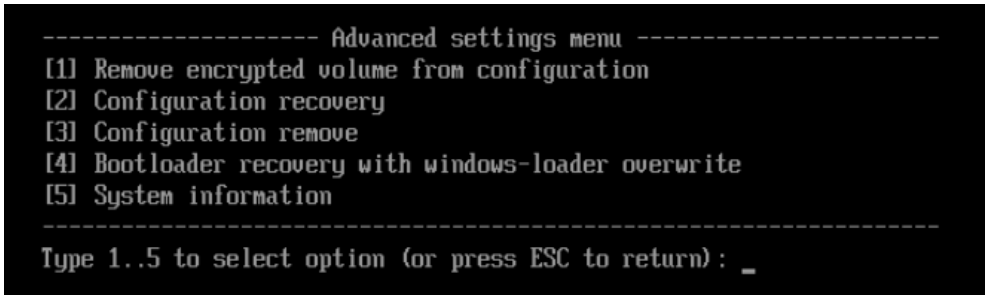


Рис.8 Меню дополнительных настроек диска аварийного восстановления Secret Net Studio

Создание диска аварийного восстановления

Создание диска аварийного восстановления выполняется с помощью утилиты SnRescue, находящейся на установочном диске Secret Net Studio.

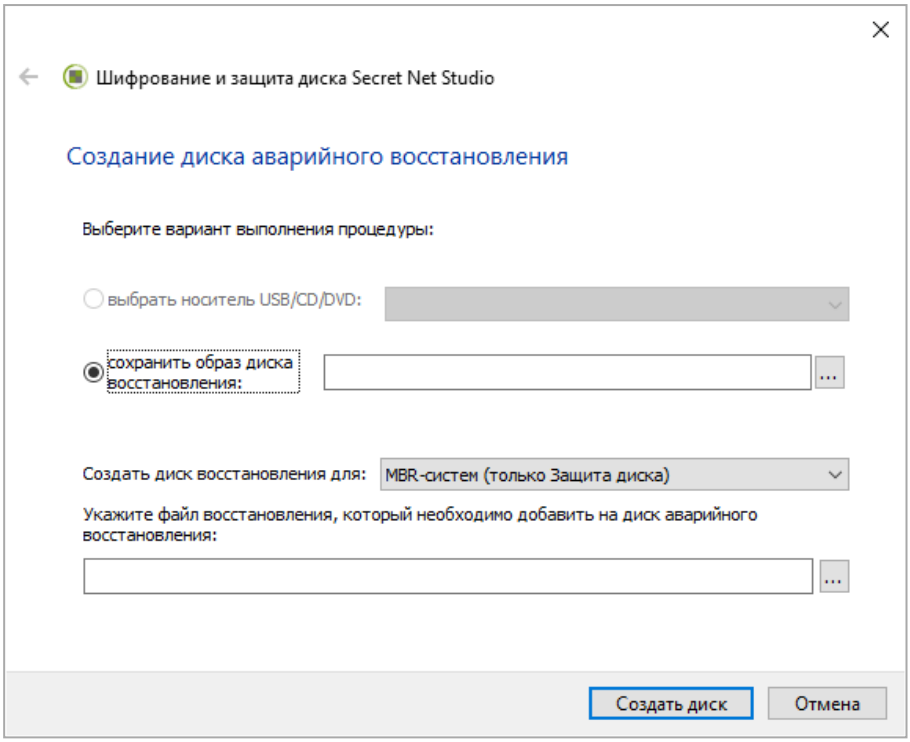
Внимание! Для создания диска, который будет использоваться для восстановления конфигурации и расшифрования данных, понадобится файл восстановления. Рекомендуется использовать файл восстановления, сохраненный после шифрования всех необходимых дисков компьютера. Сохранение файла восстановления выполняется:

- при локальном хранении данных восстановления — в мастере шифрования Secret Net Studio на компьютере с зашифрованными дисками (см. стр.195);
- при централизованном хранении данных восстановления — в Центре управления на сервере безопасности для компьютера с зашифрованными дисками (см. стр.197).

Для создания диска аварийного восстановления:

1. Запустите на исполнение от имени администратора файл утилиты:
   - для 32-разрядных ОС — \Tools\SecurityCode\SnRescue\SnRescue32.exe;
   - для 64-разрядных ОС — \Tools\SecurityCode\SnRescue\SnRescue.exe.

   На экране появится окно мастера создания диска аварийного восстановления Secret Net Studio, подобное представленному на рисунке ниже.



2. Выберите один из вариантов выполнения процедуры:
   - "выберите носитель USB/CD/DVD:" — выберите носитель, который будет являться диском аварийного восстановления;
   - "сохранить образ диска восстановления:" — укажите путь для сохранения образа диска аварийного восстановления.
3. Укажите, для какой цели и подсистемы необходимо создать диск аварийного восстановления. Для этого выберите одно из значений в раскрывающемся списке "Создать диск восстановления для:":
   - "MBR-систем (только Защита диска)" — диск будет предназначен для восстановления доступа к диску, защищенному с помощью механизма защиты диска Secret Net Studio;
   - "UEFI-систем (без файла восстановления)" — диск будет предназначен для восстановления загрузчика Secret Net Studio;
   - "UEFI-систем" — диск будет предназначен для выполнения всех операций, описанных в разделе выше.

Пояснение. Интерфейс диска аварийного восстановления для MBR-систем отличается от интерфейса для UEFI-систем.

4. При необходимости укажите путь к файлу восстановления, который необходимо добавить на диск аварийного восстановления.
5. Нажмите кнопку "Создать диск".

   На экране появится диалог, отображающий процесс создания диска аварийного восстановления. По завершении процесса отобразится сообщение с указанием пути к образу диска.
6. Нажмите кнопку "Завершить".

Смена пароля доступа к дискам

Команда предназначена для смены пароля доступа к дискам, зашифрованным с помощью механизма полнодискового шифрования Secret Net Studio.

Для смены пароля:

1. Выполните загрузку компьютера с зашифрованным диском с диска аварийного восстановления.

На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).

2. Введите номер команды "Password change" и нажмите клавишу <Enter>.

   На экране появится запрос текущего пароля доступа к дискам.

3. Введите пароль доступа к дискам и нажмите клавишу <Enter>.

   Пояснение. Для отображения символов пароля нажмите клавишу <F5>.

   Появится запрос нового пароля.

4. Введите новый пароль доступа к дискам и нажмите клавишу <Enter>.

   Пояснение. Для отображения символов пароля нажмите клавишу <F5>.

   Появится сообщение об успешной смене пароля.

5. Для возврата в главное меню диска аварийного восстановления нажмите любую клавишу.

Сброс пароля доступа к дискам

Команда предназначена для сброса пароля доступа к дискам, зашифрованным с помощью механизма полнодискового шифрования Secret Net Studio. Для сброса необходим код восстановления.

Пояснение. Код восстановления можно сохранить:

- при локальном хранении данных восстановления — в мастере шифрования Secret Net Studio на компьютере с зашифрованными дисками (см. стр.**195**);
- при централизованном хранении данных восстановления — в Центре управления на сервере безопасности для компьютера с зашифрованными дисками (см. стр.**197**).

Для сброса пароля:

1. Выполните загрузку компьютера с зашифрованным диском с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).

2. Введите номер команды "Password reset with recovery-code" и нажмите клавишу <Enter>.

   На экране отобразятся идентификатор зашифрованного диска и запрос кода восстановления.

3. Введите код восстановления, соответствующий идентификатору, и нажмите клавишу <Enter>.

   Появится запрос пароля к коду восстановления.

4. Введите пароль к коду восстановления и нажмите клавишу <Enter>.

   Пояснение. Для скрытия символов пароля нажмите клавишу <F5>.

   При успешном вводе пароля появится запрос на установку нового пароля доступа к зашифрованным дискам.

5. Введите новый пароль доступа к дискам и нажмите клавишу <Enter>.

   Пояснение. Для отображения символов пароля нажмите клавишу <F5>.

   Пароль доступа к зашифрованным дискам будет изменен.

6. Для возврата в главное меню диска аварийного восстановления нажмите любую клавишу.

Снятие защиты диска и расшифрование данных

Команда предназначена для снятия защиты диска, защищенного с помощью механизма защиты диска Secret Net Studio, а также для расшифрования данных на дисках, зашифрованных с помощью механизма полнодискового шифрования Secret Net Studio.

Для снятия защиты диска и расшифрования данных:

1. Выполните загрузку компьютера, диск которого необходимо расшифровать или с которого необходимо снять защиту, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).

2. Введите номер команды "Volume decryption" и нажмите клавишу <Enter>.

   На экране отобразится список защищенных / зашифрованных дисков компьютера.

3. Введите порядковый номер нужного диска.

   Появится запрос пароля доступа к диску.

4. Введите пароль доступа к диску и нажмите клавишу <Enter>.

   Пояснение. Для отображения символов пароля нажмите клавишу <F5>.

   При успешном вводе пароля начнется процесс снятия защиты или расшифрования.

   Пояснение. Для прерывания процесса нажмите клавишу <ESC>. На экране отобразится список защищенных / зашифрованных дисков. При выборе диска, для которого ранее была запущена операция, процесс снятия защиты или расшифрования продолжится.
   Если диск останется частично защищенным / зашифрованным, после входа в систему он будет снова полностью защищен / зашифрован.

   По окончании процесса на экране появится соответствующее сообщение.

   Пояснение. Если на компьютере имеется несколько защищенных / зашифрованных дисков и с помощью диска аварийного восстановления снята защита или расшифрованы не все диски, то после входа в систему появится запрос на сохранение нового файла восстановления.

Восстановление загрузчика Secret Net Studio

При возникновении проблем с загрузкой можно удалить и восстановить загрузчик Secret Net Studio с помощью диска аварийного восстановления. Доступны два способа восстановления:

- восстановление только загрузчика Secret Net Studio;
- восстановление загрузчика Secret Net Studio с перезаписью загрузчика ОС Windows.

Внимание! После удаления загрузчика Secret Net Studio выполните команду его восстановления. Если после восстановления возникают ошибки загрузки ОС, выполните команду восстановления загрузчика Secret Net Studio с перезаписью загрузчика ОС Windows.

Для удаления загрузчика Secret Net Studio:

1. Выполните загрузку компьютера, на котором необходимо восстановить загрузчик Secret Net Studio, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).

2. Введите номер команды "Bootloader remove" и нажмите клавишу <Enter>.

   Появится запрос на подтверждение операции.

3. Введите команду "y" и нажмите клавишу <Enter>.

   Отобразится информация об удалении загрузчика Secret Net Studio с указанием удаляемых файлов. Далее появится сообщение об успешном удалении загрузчика.

4. Для возврата в главное меню диска аварийного восстановления нажмите любую клавишу.

Для восстановления загрузчика Secret Net Studio:

1. Выполните загрузку компьютера, на котором необходимо восстановить загрузчик Secret Net Studio, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).
2. Введите номер команды "Bootloader recovery" и нажмите клавишу <Enter>.

   Появится запрос на подтверждение операции.
3. Введите команду "y" и нажмите клавишу <Enter>.

   Появится сообщение об успешном восстановлении загрузчика Secret Net Studio.
4. Для возврата в главное меню диска аварийного восстановления нажмите любую клавишу.

Для восстановления загрузчика Secret Net Studio с перезаписью загрузчика ОС Windows:

1. Выполните загрузку компьютера, на котором необходимо восстановить загрузчик Secret Net Studio, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).
2. Введите номер команды "Advanced settings" и нажмите клавишу <Enter>.

   Появится меню дополнительных настроек (см. Рис.8 на стр.**300**).
3. Введите номер команды "Bootloader recovery with windows-loader overwrite" и нажмите клавишу <Enter>.

   Появится запрос на подтверждение операции.
4. Введите команду "y" и нажмите клавишу <Enter>.

   Появится сообщение об успешном восстановлении загрузчика.
5. Для возврата в меню дополнительных настроек диска аварийного восстановления нажмите любую клавишу.

Восстановление конфигурации защитных подсистем

Команда предназначена для восстановления файла конфигурации подсистем защиты диска и полнодискового шифрования Secret Net Studio. Выполняется замена имеющегося на компьютере файла конфигурации на файл, размещенный на диске аварийного восстановления. Сохраняется резервная копия имеющегося на компьютере файла конфигурации.

Внимание! При использовании диска аварийного восстановления с неактуальным файлом восстановления команда восстановления конфигурации может привести к потере данных на защищенных / зашифрованных дисках.

Во избежание потери данных при создании диска аварийного восстановления необходимо использовать файл восстановления, сохраненный после шифрования всех необходимых дисков компьютера.

Для восстановления конфигурации защитных подсистем:

1. Выполните загрузку компьютера, на котором необходимо восстановить конфигурацию защитных подсистем, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).
2. Введите номер команды "Advanced settings" и нажмите клавишу <Enter>.

   Появится меню дополнительных настроек (см. Рис.8 на стр.**300**).
3. Введите номер команды "Configuration recovery" и нажмите клавишу <Enter>.

   Осуществится поиск файла восстановления на диске аварийного восстановления.

Пояснение. Если файл восстановления не найден, повторите процедуру создания диска аварийного восстановления с опцией записи на него файла восстановления (см. стр.**300**).

Если файл найден, появится запрос на перезапись файла конфигурации.

4. Введите команду "y" и нажмите клавишу <Enter>.

   Файл конфигурации защитных подсистем будет перезаписан. На экране появится сообщение с указанием пути сохранения резервной копии прежнего файла конфигурации.

5. Для возврата в меню дополнительных настроек диска аварийного восстановления нажмите любую клавишу.

Удаление конфигурации защитных подсистем

Команда предназначена для удаления файла конфигурации подсистем защиты диска и полнодискового шифрования Secret Net Studio. В результате выполнения операции после перезагрузки компьютера создается новый пустой файл конфигурации, если не удален загрузчик Secret Net Studio. Сохраняется резервная копия имеющегося на компьютере файла конфигурации.

Внимание! Команда удаления файла конфигурации может привести к потере доступа к данным на зашифрованных / защищенных дисках. В этом случае восстановить доступ к данным можно только при наличии актуального файла восстановления с помощью команды восстановления файла конфигурации (см. стр.**304**). Настоятельно рекомендуется применять команду удаления файла конфигурации защитных подсистем только при повреждении данного файла (по причине ошибок на диске, попытки подмены файла злоумышленниками и т.д.).

Для удаления конфигурации защитных подсистем:

1. Выполните загрузку компьютера, на котором необходимо восстановить конфигурацию защитных подсистем, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).

2. Введите номер команды "Advanced settings" и нажмите клавишу <Enter>.

   Появится меню дополнительных настроек (см. Рис.8 на стр.**300**).

3. Введите номер команды "Configuration remove" и нажмите клавишу <Enter>.

   Появится запрос на подтверждение операции.

4. Введите команду "y" и нажмите клавишу <Enter>.

   Файл конфигурации защитных подсистем будет удален. На экране появится сообщение с указанием пути сохранения резервной копии файла конфигурации.

5. Для возврата в меню дополнительных настроек диска аварийного восстановления нажмите любую клавишу.

Удаление зашифрованного диска из конфигурации

В случае повреждения одного из зашифрованных несистемных разделов на жестком диске с несколькими зашифрованными разделами можно удалить из конфигурации информацию о поврежденном разделе. Тогда будут потеряны зашифрованные данные только на поврежденном разделе; на остальных разделах данные будут доступны.

Пояснение. Команда удаления зашифрованного диска из конфигурации может помочь, например, в следующих ситуациях:

- Жесткий диск с зашифрованными разделами установили в другой компьютер, отформатировали зашифрованный раздел и записали на него новые данные. Для сохранения новых данных и данных на других зашифрованных разделах можно воспользоваться указанной командой на компьютере, на котором разделы были зашифрованы. Отформатированный раздел уже не будет считаться зашифрованным.
- Повреждена конфигурация подсистемы полнодискового шифрования. Если удалось выяснить, для какого именно зашифрованного раздела поврежден файл конфигурации, можно воспользоваться указанной командой для сохранения данных на других зашифрованных разделах.
- Конфигурация зашифрованного раздела была изменена (изменен размер, раздел удален и др.). Для сохранения данных на других зашифрованных разделах можно воспользоваться указанной командой.

Для удаления зашифрованного диска из конфигурации:

1. Выполните загрузку компьютера, на котором необходимо восстановить конфигурацию защитных подсистем, с диска аварийного восстановления.

   На экране появится главное меню диска аварийного восстановления Secret Net Studio (см. Рис.7 на стр.**300**).
2. Введите номер команды "Advanced settings" и нажмите клавишу <Enter>.

   Появится меню дополнительных настроек (см. Рис.8 на стр.**300**).
3. Введите номер команды "Remove encrypted volume from configuration" и нажмите клавишу <Enter>.

   На экране отобразится список зашифрованных дисков компьютера.
4. Введите порядковый номер нужного диска.

   Появится запрос на подтверждение операции.
5. Введите команду "y" и нажмите клавишу <Enter>.

   Информация о выбранном зашифрованном разделе будет удалена из конфигурации подсистемы полнодискового шифрования.
6. Для возврата в меню дополнительных настроек диска аварийного восстановления нажмите любую клавишу.

Рекомендации по настройке Secret Net Studio на кластере

Кластерные технологии позволяют объединить группу компьютеров (узлов), независимо работающих под управлением своих ОС, в единый сервер. При настройке клиентов системы Secret Net Studio, установленных на кластер, учитывайте следующие рекомендации:

1. Все службы клиентского ПО должны постоянно работать на всех узлах кластера, включая неактивные. Эти службы не следует кластеризовать, то есть включать в ресурс, которым управляет сервис кластеров. Иначе при переключении будет потеряна работоспособность системы защиты на неактивных узлах, а механизм функционального контроля заблокирует работу кластера, определив отсутствие базовых защитных подсистем.
2. Общий ресурс (физический диск или сетевой адаптер) в списке устройств Secret Net Studio следует перевести в режим "Подключение устройства разрешено" или "Устройство не контролируется". Если для такого ресурса включен режим "Устройство постоянно подключено к компьютеру" (включен по умолчанию для физических дисков и сетевых адаптеров), может фиксироваться нарушение аппаратной конфигурации при переключении ресурса во время работы механизма контроля.

   Примечание. Аналогичная особенность может проявляться и на одиночном компьютере, на котором установлены несколько SCSI-дисков.
3. Не следует включать контроль целостности для файлов, размещенных на общем ресурсе. Это вызвано тем, что при переходе узла кластера в неактивное состояние он теряет доступ к общему ресурсу. В случае если для данного узла процедура контроля была предусмотрена, в момент ее проведения будет зафиксировано нарушение целостности объектов, поставленных на контроль.
4. При настройке замкнутой программной среды для пользователя не следует указывать локальный путь для исполняемых файлов, размещенных на общем ресурсе кластера. В этом случае необходимо использовать сетевые пути для разрешенных исполняемых модулей.
5. Для автономного режима функционирования клиента Secret Net Studio необходимо установить на всех узлах кластера тождественные настройки доменных пользователей. В противном случае работа системы Secret Net Studio будет различаться в зависимости от того, какой узел активен. Данная рекомендация актуальна, в частности, для механизма полномочного управления доступом, поскольку этот механизм обрабатывает сетевые обращения к файлам и определяет возможность доступа к ним, используя настройки пользователей, размещенные в локальной базе данных на кластере.

Восстановление системы после сбоев питания компьютера

В большинстве случаев внезапное отключение питания компьютера не приводит к потере работоспособности системы Secret Net Studio при следующих запусках. Однако возможны ситуации, когда после сбоя питания происходит блокировка компьютера или другие проявления нештатного поведения системы.

В таких случаях проблемы могут возникать из-за повреждения следующих функциональных компонентов системы защиты:

- база данных КЦ-ЗПС;
- локальная база данных системы Secret Net Studio;
- программные модули системы Secret Net Studio.

Ниже приводится порядок действий администратора для восстановления работоспособности БД КЦ-ЗПС и ЛБД системы защиты. В дальнейшем для решения проблемы рекомендуется добавить подкаталоги \Icheck и \GroupPolicy, находящиеся в каталоге установки Secret Net Studio, в список исключений из проверки антивирусом. Если описанные действия не приводят к устранению проблем, переустановите на компьютере ПО системы Secret Net Studio (см. документ [**1**]). При дальнейших проявлениях нештатного поведения системы обратитесь в отдел технической поддержки компании "Код Безопасности".

Восстановление базы данных КЦ-ЗПС

При повреждении БД КЦ-ЗПС система во время загрузки компьютера продолжительное время ожидает старта подсистемы контроля целостности. Время ожидания может длиться до одного часа. Также для этих случаев характерны ошибки функционального контроля, сообщающие об отсутствии подсистемы КЦ-ЗПС.

Для восстановления БД КЦ-ЗПС:

- Удалите каталог \icheck, расположенный в каталоге установки компонента "Secret Net Studio", и перезагрузите компьютер.

  После восстановления БД КЦ-ЗПС локальные параметры механизмов КЦ и ЗПС будут приведены в состояние по умолчанию. При загрузке компьютера автоматически выполняется синхронизация, в результате которой на компьютер загружаются централизованно заданные параметры. Ранее заданные локальные параметры потребуется восстановить вручную.

Восстановление локальной базы данных

При повреждении локальной базы данных системы Secret Net Studio во время загрузки компьютера возникают ошибки функционального контроля, сообщающие об отсутствии или неработоспособности ядра системы защиты.

Для восстановления локальной БД:

1. Запустите консоль командной строки (cmd.exe).
2. Перейдите в каталог \GroupPolicy, расположенный в каталоге установки компонента "Secret Net Studio".
3. Последовательно введите команды:
   - del *.chk
   - del *.log
   - del *.edb
4. Введите команду esentutl /p snet.sdb (на запрос ответить "OK").
5. Снова введите команды del *.chk, del *.log и del *.edb.
6. Перезагрузите компьютер.

   После восстановления локальной БД параметры Secret Net Studio в локальной политике безопасности будут приведены в состояние по умолчанию. При загрузке компьютера автоматически применяются централизованно заданные параметры в соответствии с действием групповых политик. Параметры политики безопасности, ранее заданные локально, потребуется восстановить вручную.

Ошибки и предупреждения при работе с ДС

Предупреждения в программе управления

Параметр "Состояние" в окне со сведениями о подсистеме "Доверенная среда" (см. Рис.1 на стр.**253**) отражает информацию о соответствии / несоответствии компьютера системным требованиям для установки ДС. Данную информацию можно просмотреть в локальном и централизованном режимах.

При несоответствии компьютера системным требованиям параметр может принимать значения из таблицы ниже.

Текст ошибки
Версия операционной системы ниже, чем требуется
Число процессоров ниже, чем требуется
Поддержка виртуализации отключена
Second Level Address Translation не поддерживается аппаратным обеспечением
Используемый тип диска (NVMe, VHD и т.п.) не поддерживается
Работа в виртуальном окружении не поддерживается
Обнаружено несовместимое оборудование

Ошибки при включении компьютера

При включении компьютера с ДС, функционирующей в жестком режиме, может возникнуть системная ошибка BSOD. Причиной такой ошибки может являться компьютерная атака и другие нарушения безопасности информации. При невозможности самостоятельно справиться с проблемой обратитесь в департамент сервиса компании "Код Безопасности".

Коды системных ошибок BSOD, связанных с ДС, и их краткое описание приведены в таблице ниже.

Код ошибки	Пояснение
0x5ECC0DE0	Нарушение целостности процессов Secret Net Studio
0x5ECC0DE1	Ошибка инициализации драйвера ДС
0x5ECC0DE2	Сброс регистра SMEP
0x5ECC0DE3	Ошибка КС драйвера
0x5ECC0DE4	Попытка модификации драйвера
0x5ECC0DE5	Выгрузка драйвера
0x5ECC0DE6	Несанкционированное завершение процесса
0x5ECC0DE7	Срабатывание сторожевого таймера для процесса
0x5ECC0DE8	Ошибка КС процесса
0x5ECC0DE9	Атака 0-го кольца
0x5ECC0DEA	Внутренняя ошибка драйвера ДС

Объекты КЦ ДС по умолчанию

При включении ДС автоматически ставятся на контроль драйверы, службы и приложения Secret Net Studio. Перечень этих файлов приведен в таблице ниже.

Полное имя файла	Тип файла
SystemRoot\System32\Drivers\Sn5CrPack.sys	Драйвер
SystemRoot\System32\Drivers\Sn5Crypto.sys	Драйвер
SystemRoot\System32\Drivers\SnCC0.sys	Драйвер
SystemRoot\System32\Drivers\SnCDFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnCloneVault.sys	Драйвер
SystemRoot\System32\Drivers\SnDacs.sys	Драйвер
SystemRoot\System32\Drivers\SnDDD.sys	Драйвер
SystemRoot\System32\Drivers\SnDeviceFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnDiskEnc.sys	Драйвер
SystemRoot\System32\Drivers\SnDiskFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnEraser.sys	Драйвер
SystemRoot\System32\Drivers\SnExeQuota.sys	Драйвер
SystemRoot\System32\Drivers\SnFDac.sys	Драйвер
SystemRoot\System32\Drivers\SnFileControl.sys	Драйвер
SystemRoot\System32\Drivers\SnFMac.sys	Драйвер
SystemRoot\System32\Drivers\SnNetFlt.sys	Драйвер
SystemRoot\System32\Drivers\snsdp.sys	Драйвер
SystemRoot\System32\Drivers\SnTmCardDrv.sys	Драйвер
SystemRoot\System32\Drivers\SnWiper0.sys	Драйвер
SystemRoot\System32\Drivers\ScTeDrv.sys	Драйвер
SystemRoot\System32\Drivers\SCTEFsFlt.sys	Драйвер
%ClientInstallDir%\SnSrv.exe	Служба
%ClientInstallDir%\SnicheckSrv.exe	Служба
%ClientInstallDir%\SnIcon.exe	Приложение

Ограничения и рекомендации при работе с ДС

ДС является новым защитным механизмом Secret Net Studio, который находится в стадии активной разработки. В данном разделе приведены ограничения и рекомендации по использованию ДС в текущей реализации (Secret Net Studio версии 8.5).

Несовместимое оборудование и конфигурации

Ниже перечислены особенности функционирования ДС с различным оборудованием, которые актуальны даже при соответствии компьютера минимальным системным требованиям, приведенным на стр.**251**.

1. Виртуальная среда.

   ДС функционирует только при одном работающем гипервизоре, виртуальное окружение не поддерживается. Для использования ДС необходим физический компьютер.

   Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.

2. Жесткие диски.
   - В текущей реализации ДС функционирует только с жесткими дисками SATA/AHCI.

     Работа с дисками SCSI, NVMe, а также с образами дисков VHD1 (и другими разновидностями) не поддерживается.

     Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.
   - Рекомендуется использовать жесткий диск в режиме AHCI. Работа с жестким диском в режиме IDE нестабильна.
   - В текущей реализации не поддерживаются RAID-конфигурации и полнодисковое шифрование.
   - Не рекомендуется использовать ДС на конфигурации с несколькими ОС, так как в текущей реализации не обеспечивается запуск той ОС, в которой настроена ДС.
3. Системные платы.

   Системная плата Gigabyte H67A-UD3H-B3 с версией UEFI/BIOS F81 не поддерживается из-за некорректной работы с контроллером диска.

   Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.
4. USB-контроллеры.
   - Наблюдается нестабильная работа с контроллером USB 3.1. Используйте контроллеры USB 3.0/2.0 при подключении загрузочного носителя ДС.
   - Подключение нескольких загрузочных USB-флеш-накопителей не поддерживается. Подключайте только загрузочный носитель ДС до включения компьютера.
5. Процессоры.

   На платформе AMD было проведено ограниченное тестирование ДС. Полное функционирование механизма не гарантируется.

Рекомендации по настройке компьютера

Ниже приведены рекомендации по настройке компьютера для обеспечения корректного функционирования ДС.

1. UEFI/BIOS.
   - Рекомендуется обновить UEFI/BIOS до последней версии.
   - В UEFI/BIOS Setup необходимо разрешить использование всех функций виртуализации. Как правило, параметры виртуализации находятся в разделе "CPU configuration".
   - В UEFI/BIOS Setup необходимо разрешить использование CSM (Compatibility Support Module). В настройках CSM рекомендуется выбрать режим "UEFI and Legacy".

     Примечание. При отсутствии в настройках CSM режима "UEFI and Legacy" необходимо выбрать режим "Legacy".
   - В UEFI/BIOS Setup в настройках USB рекомендуется активировать параметры "Full Initialization" и "USB boot first" (при наличии таких параметров).
2. Жесткий диск.
   - Не рекомендуется использовать жесткий диск с ошибками S.M.A.R.T., так как работа с таким диском нестабильна.
   - Не поддерживается работа с жестким диском с включенным аппаратным шифрованием.

Примечание. Если жесткий диск поддерживает функцию аппаратного шифрования, отключите данную функцию. Работа с диском будет осуществляться так же, как с диском без функции аппаратного шифрования.

3. ОС семейства Windows.

   Спящий режим в ОС семейства Windows приводит к нестабильной работе. Рекомендуется настроить следующие параметры с помощью powercfg.cpl:

   - отключить спящий режим;
   - для процессора установить все режимы 100%;
   - запретить отключение системного жесткого диска.

Очистка загрузочного носителя ДС

Для использования всего объема памяти USB-флеш-накопителя, применяемого ранее в качестве загрузочного носителя ДС, необходимо выполнить полную очистку USB-флеш-накопителя с помощью стандартной утилиты управления дисками ОС Windows *diskpart.exe*.

Внимание! При полной очистке все данные на USB-флеш-накопителе будут уничтожены. Чтобы снова использовать USB-флеш-накопитель для работы с ДС, выполните процедуру создания загрузочного носителя со стр.252.

Для очистки загрузочного носителя ДС:

1. Подключите загрузочный носитель ДС к компьютеру.
2. Запустите утилиту командной строки ОС Windows от имени администратора.
3. Выполните следующую команду:

   ```
   diskpart
   ```

   Запустится утилита *diskpart.exe*.
4. Выполните следующую команду:

   ```
   list disk
   ```

   Отобразится список дисков, подключенных к компьютеру.
5. Найдите в списке нужный USB-флеш-накопитель и запомните его номер.
6. Выполните следующие команды:

   ```
   select disk <номер диска>
   clean
   create partition primary
   ```

   USB-флеш-накопитель будет очищен. На носителе будет создан первичный раздел.
7. Выполните форматирование USB-флеш-накопителя в нужную файловую систему любым удобным способом.

Документация

1. Средство защиты информации Secret Net Studio – C. Руководство администратора. Установка, управление, мониторинг и аудит	RU.88338853.501400.002 91 1
2. Средство защиты информации Secret Net Studio – C. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.002 91 2
3. Средство защиты информации Secret Net Studio – C. Руководство пользователя	RU.88338853.501400.002 92