КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Настройка и эксплуатация

RU.88338853.501400.001 91 3

Оглавление

Список сокращений

AD	Active Directory
CRC	Cyclic Redundancy Check
DNS	Domain Name System
FAT	File Allocation Table
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long File Name
MMC	Microsoft Management Console
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RPC	Remote Procedure Call
RTF	Rich Text Format
SID	Security Identifier
TCP	Transmission Control Protocol
USB	Universal Serial Bus
АРМ	Автоматизированное рабочее место
БД	База данных
ЗПС	Замкнутая программная среда
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
ЦБД	Центральная база данных
ЭЦП	Электронная цифровая подпись

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для настройки и управления механизмами защиты, входящими в состав базовой защиты изделия. Перед изучением данного руководства необходимо 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. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

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

Глава 1
Основные сведения о настройке и эксплуатации

В Secret Net Studio информационная безопасность компьютеров обеспечивается механизмами защиты. Механизмы реализуют различные возможности разграничения доступа к ресурсам и контроль действий пользователей. Описание механизмов защиты Secret Net Studio приведено в документе [**1**].

Организация управления системой защиты

Централизованное и локальное управление

Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на компьютере. Локальное управление используется в тех случаях, когда возможности централизованного управления для отдельного компьютера недоступны или нецелесообразны. Например, если требуется обеспечить безопасную работу локальных пользователей компьютера. Программные средства локального управления установлены по умолчанию и могут использоваться пользователями, входящими в локальную группу администраторов компьютера.

Централизованное управление параметрами Secret Net Studio осуществляется администратором безопасности со своего рабочего места. Для этих целей может использоваться любой компьютер сети с установленными средствами централизованного управления.

В автономном режиме функционирования клиента Secret Net Studio доступны только возможности локального управления. В сетевом режиме управление можно осуществлять как локально, так и централизованно.

Внимание!
В соответствии с концепцией Secret Net Studio управление работой защищаемых компьютеров с установленным клиентом в сетевом режиме функционирования рекомендуется осуществлять централизованно. Централизованное управление имеет приоритет перед локальным управлением. Например, если в групповой политике некоторые параметры заданы централизованно, то локально на компьютере их изменить нельзя.

Использование групповых политик

Для централизованной настройки и применения параметров безопасности на защищаемых компьютерах с установленным клиентом в сетевом режиме функционирования могут использоваться групповые политики. По умолчанию параметры заданы только в локальной политике, имеющей наименьший приоритет.

В дополнение к параметрам локальной политики могут быть заданы параметры в политиках доменов, организационных подразделений и серверов безопасности. Эти параметры применяются на компьютерах, которые относятся к соответствующим доменам, организационным подразделениям или серверам безопасности, независимо от заданных значений в локальной политике каждого компьютера.

Параметры групповых политик применяются в следующей последовательности:

- локальная политика;
- политика домена;
- политика организационного подразделения — применяется на всех компьютерах, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности — применяется на всех компьютерах, подчиненных этому серверу безопасности.

При наличии иерархии серверов безопасности параметры политик этих серверов применяются последовательно — начиная с сервера, которому компьютеры подчинены непосредственно, и далее до корневого сервера в иерархии. Таким образом, параметры, заданные в политике корневого сервера безопасности, имеют наивысший приоритет.

Настройка параметров групповых политик осуществляется в программе управления системы Secret Net Studio. Сведения о работе с программой управления см. в документе [**4**].

За счет использования разных групповых политик реализуется централизованное управление параметрами с учетом особенностей информационной системы. Например, можно настроить общие параметры для всех компьютеров в политике домена и дополнительно указать значения отдельных параметров в политиках организационных подразделений. Это позволит применять на компьютерах различных организационных подразделений единые общие параметры и при этом задать специфические значения для компьютеров отдельных подразделений.

Обновление групповых политик

Параметры групповых политик на защищаемых компьютерах обновляются автоматически, в соответствии с действием механизма применения политик ОС Windows. При необходимости администратор может использовать средства принудительного обновления политик, чтобы ускорить процесс применения централизованно заданных параметров на компьютерах.

Принудительное обновление групповых политик можно осуществлять с помощью следующих средств:

- команда применения групповых политик в программе управления;
- стандартные инструменты командной строки gpudate и secedit.

После обновления политик может потребоваться перезапуск компьютера или завершение текущего сеанса работы пользователя — чтобы применить параметры, которые действуют только при загрузке ОС или при входе пользователя в систему. Для этого предусмотрены специальные возможности как в программе управления (команды для перезагрузки или выключения компьютеров), так и в указанных инструментах командной строки.

Делегирование административных полномочий

Делегирование позволяет передать некоторые функции по настройке и управлению пользователям, не входящим в доменную группу администраторов.

По умолчанию администраторы безопасности обладают всеми необходимыми полномочиями для настройки параметров механизмов защиты Secret Net Studio. Однако некоторые функции управления объектами, доступные администраторам домена, также могут потребоваться и администраторам безопасности для выполнения своих служебных обязанностей. В частности, административная смена паролей пользователей, создание и удаление пользователей и групп пользователей, а также настройка основных параметров учетных записей. Чтобы предоставить администраторам безопасности эти возможности, администратор домена может делегировать соответствующие задачи с помощью стандартных средств ОС Windows.

Процедура делегирования выполняется в оснастке "Active Directory — пользователи и компьютеры" с использованием специального мастера делегирования управления. Запуск мастера нужно выполнить для соответствующего контейнера AD — всего домена или отдельного организационного подразделения (в зависимости от того, какими объектами разрешено управлять администратору безопасности). В мастере делегирования укажите учетную запись администратора безопасности или группы и затем в списке задач установите отметки для следующих элементов:

- "Создание, удаление и управление учетными записями пользователей" (Create, delete, and manage user accounts);

- "Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке" (Reset user passwords and force password change at next logon);
- "Создание, удаление и управление группами" (Create, delete, and manage groups) — задача делегируется для организационных подразделений;
- "Изменение членства в группах" (Modify the membership of a group).

Обзор средств управления

Управление системой Secret Net Studio осуществляется с помощью специальных программных средств, устанавливаемых при развертывании системы. Средства управления предоставляют возможности для настройки системы и изменения состояния объектов, а также для контроля функционирования защищаемых компьютеров. В зависимости от назначения средства управления могут представлять собой отдельные программы или программные элементы, встраиваемые в другие средства в качестве дополнительных расширений.

Средства только для локального управления

Средства локального управления используются при работе пользователей и администраторов на защищаемом компьютере. Эти средства предназначены для выполнения действий, доступных только при локальном управлении (например, настройка параметров доступа к локальным ресурсам), для просмотра централизованно заданных параметров и для настройки тех параметров, которые не были заданы централизованно.

В состав средств, используемых только для локального управления, входят следующие программные средства:

- пиктограмма Secret Net Studio в Панели задач Windows;
- диалог "Secret Net Studio" в диалоговом окне настройки свойств ресурса;
- программа дополнительной настройки подсистемы полномочного управления доступом;
- диалоговое окно "Управление Secret Net Studio" в Панели управления Windows.

Также при локальном администрировании могут использоваться следующие средства для централизованного и локального управления:

- программа управления в локальном режиме (устанавливается в составе клиента Secret Net Studio);
- программа управления пользователями (для настройки параметров локальных пользователей);
- программа "Контроль программ и данных" в локальном режиме работы.

Примечание.
В данном разделе перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится в соответствующих документах.

Пиктограмма Secret Net Studio

После установки клиентского ПО в системной области панели задач Windows появляется пиктограмма Secret Net Studio. Пиктограмма предназначена для оповещения пользователя о наличии действующей защиты, для запуска основных пользовательских команд управления и получения сведений. Запуск команд осуществляется из контекстного меню пиктограммы. Перечень предусмотренных команд представлен в таблице.

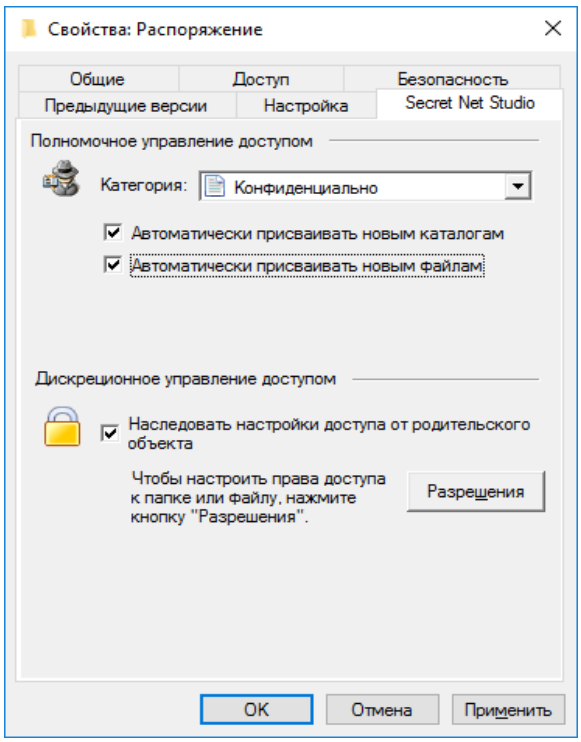
Команда	Описание
О системе	Предоставляет общую информацию о системе Secret Net Studio

Команда	Описание
Управление (для пользователя)	Вызывает локальный центр управления с правами учетной записи текущего пользователя
Управление (для администратора)	Вызывает локальный центр управления с правами встроенной учетной записи администратора компьютера
Удаление данных	Содержит команду для безвозвратного затирания всей информации на локальных носителях (см. документ [**5**])
Антивирус	Содержит команду для просмотра результатов проверок на наличие вредоносных программ, выполненных пользователем командами контекстного сканирования в программе "Проводник" в текущем сеансе работы (см. документ [**7**])
Ключи пользователя	Содержит команды для управления ключевой информацией пользователя, размещенной на ключевых носителях (см. документ [**5**])
Сбросить состояние тревоги	Выполняет сброс счетчиков событий тревоги (см. документ [**4**])
Уведомления о тревогах	Включает или отключает уведомления о событиях тревоги (см. документ [**4**])

Диалог "Secret Net Studio" в окне настройки свойств ресурса

Стандартное диалоговое окно настройки свойств ресурса (каталога или файла) ОС Windows содержит дополнительный диалог "Secret Net Studio". В диалоге выполняются действия по изменению категории конфиденциальности ресурсов для механизма полномочного управления доступом или прав доступа к ресурсам для механизма дискреционного управления доступом. Настройку может выполнять администратор безопасности или пользователи, являющиеся администраторами выбранного ресурса.

Вызов диалогового окна настройки свойств каталога или файла осуществляется стандартным способом в программе "Проводник". На рисунке представлен пример диалога "Secret Net Studio" в диалоговом окне настройки свойств каталога.

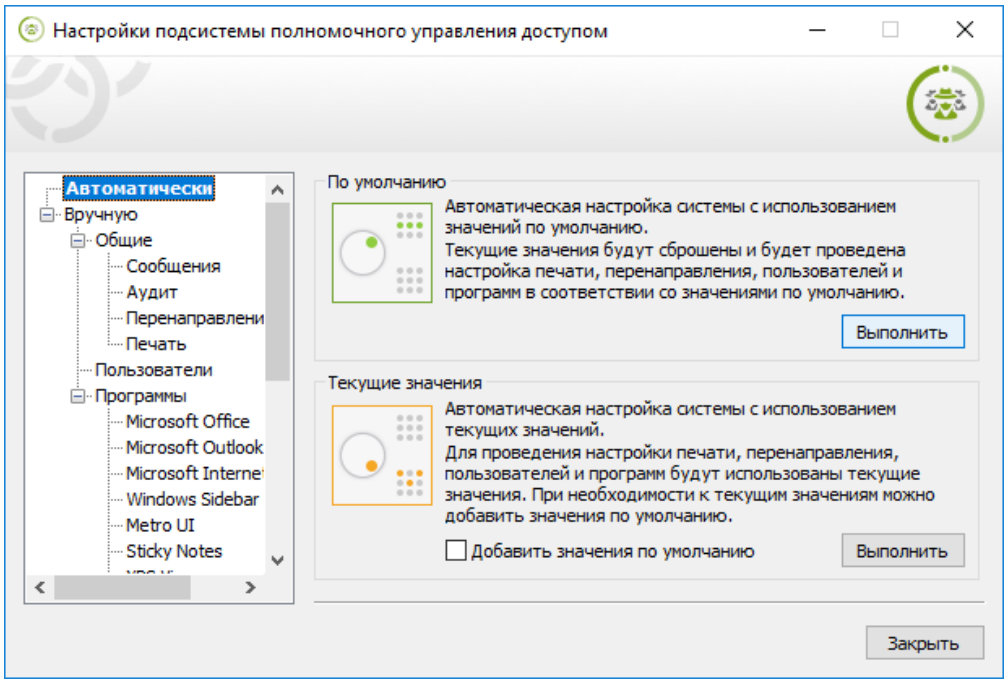


Программа настройки подсистемы полномочного управления доступом

Программа настройки подсистемы полномочного управления доступом предназначена для дополнительной настройки системы при необходимости использования режима контроля потоков. Также с помощью программы можно отключить вывод предупреждающих сообщений и регистрацию событий для случаев, когда такие оповещения не требуются.

Для запуска программы в меню "Пуск" ОС Windows в группе "Код безопасности" выберите элемент "Программа настройки подсистемы полномочного управления доступом".

Пример содержимого окна программы представлен на следующем рисунке.

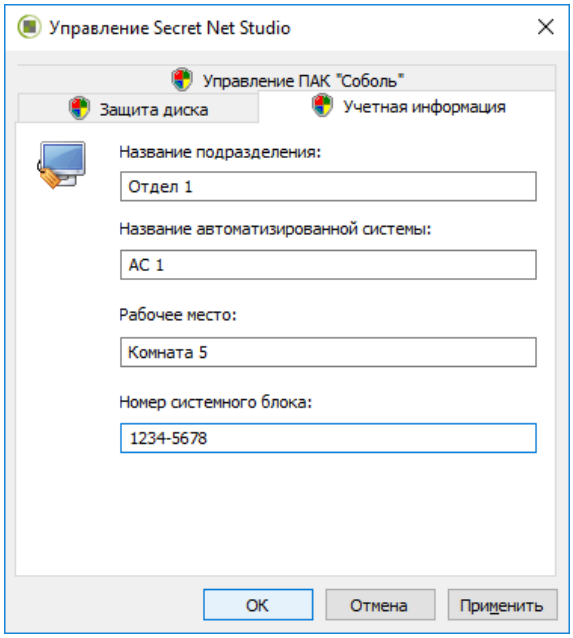


Настройка подсистемы полномочного управления доступом выполняется администратором.

Диалоговое окно "Управление Secret Net Studio" в Панели управления Windows

Диалоговое окно "Управление Secret Net Studio" предназначено для просмотра и редактирования общей информации о системе и для локального управления функционированием защитных механизмов и аппаратных средств защиты.

Вызов диалогового окна осуществляется из Панели управления ОС Windows.



Средства для централизованного и локального управления

На рабочих местах администраторов для централизованной настройки и контроля работы защищаемых компьютеров используются средства централизованного управления. При запуске в соответствующем режиме эти средства могут использоваться и для локального управления непосредственно на защищаемых компьютерах. Например, для управления компьютером с установленным клиентом Secret Net Studio в автономном режиме функционирования.

В состав средств централизованного управления входят следующие программные средства:

- программа управления;
- программа управления пользователями;
- программа "Контроль программ и данных".

Примечание.
В данном разделе перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится в соответствующих документах.

Программа управления

Программа управления устанавливается как отдельный компонент "Secret Net Studio — Центр управления" — для работы в централизованном режиме или как составная часть клиента Secret Net Studio — для работы в локальном режиме.

При работе в централизованном режиме программа предоставляет возможности управления защищаемыми компьютерами на рабочем месте администратора безопасности, мониторинга и просмотра журналов, поступивших на хранение в базу данных сервера безопасности. Для работы с программой необходимо выполнить подключение к серверу безопасности. Также предусмотрена возможность запуска без соединения с сервером безопасности — для работы с записями журналов, сохраненных в файлах.

В локальном режиме работы программы управления доступны функции только локального управления компьютером, просмотра локальных журналов и журналов, сохраненных в файлах.

Для запуска программы в централизованном режиме:

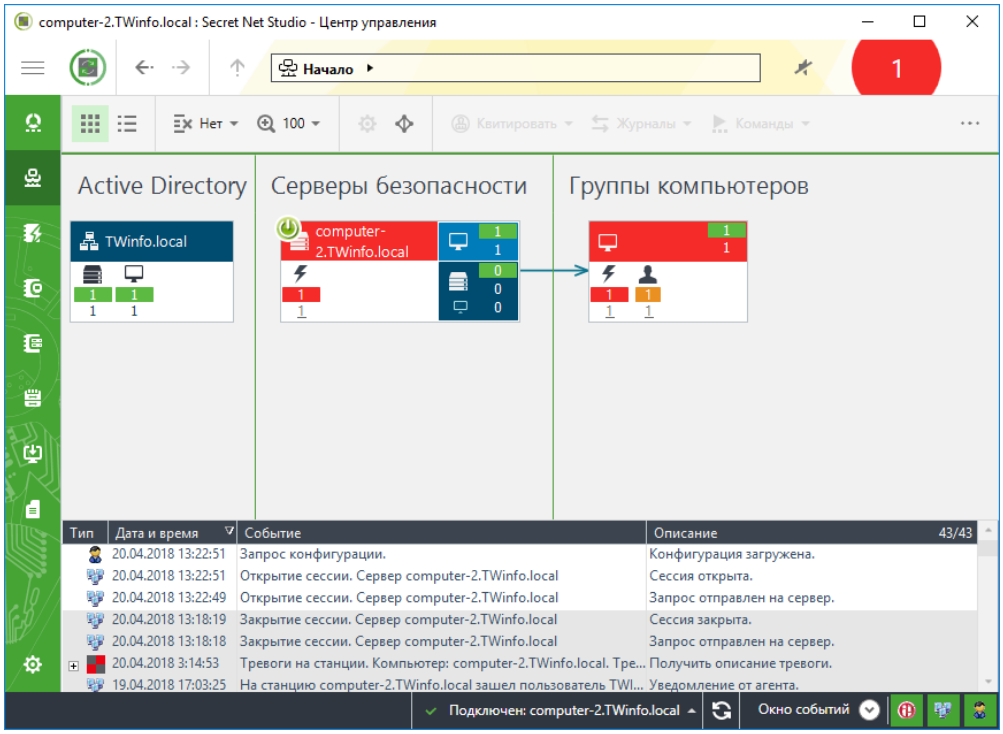
- в меню "Пуск" ОС Windows в группе "Код безопасности" выберите элемент "Центр управления".

Перед началом работы на экране появляется стартовый диалог программы, предназначенный для выбора сервера безопасности, с которым будет установлено соединение.

Для запуска программы в локальном режиме:

- в меню "Пуск" ОС Windows в группе "Код безопасности" выберите элемент "Локальный центр управления".

На рисунке представлен пример основного окна программы в централизованном режиме работы.



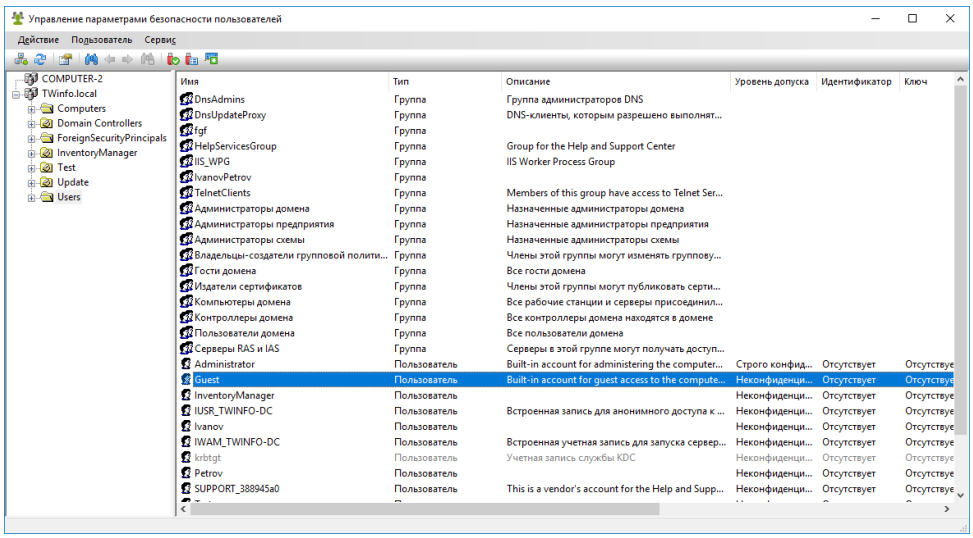
Сведения о программе управления см. в документе [**4**].

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".

Пример содержимого окна программы представлен на следующем рисунке.



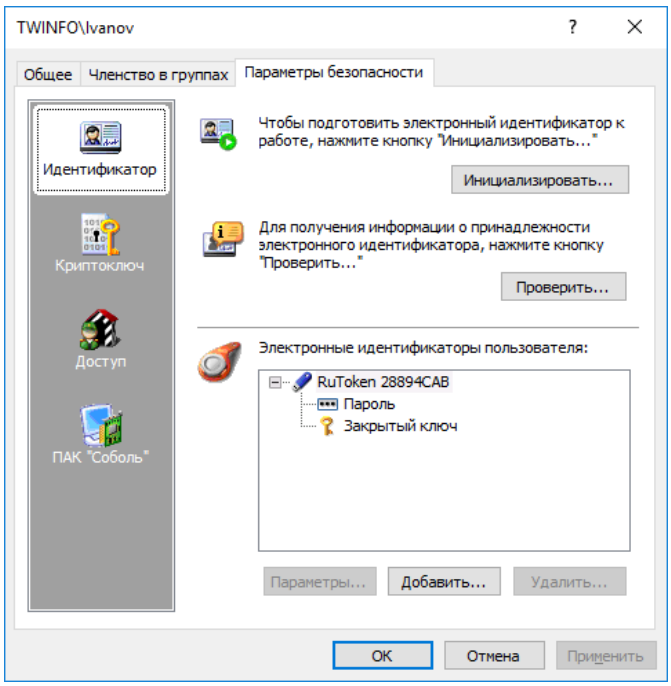
Интерфейс программы реализован аналогично стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры". В левой части окна отображается список контейнеров (текущий компьютер и структура разделов и организационных подразделений домена), а в правой — список пользователей в выбранном контейнере. Список пользователей представлен в виде таблицы со сведениями об уровнях допуска пользователей, наличии идентификаторов и криптографических ключей.

Для централизованного управления по умолчанию в программу загружается структура текущего домена. При необходимости можно загрузить структуры других доменов Active Directory, 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".

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.



Программа "Контроль программ и данных"

Программа "Контроль программ и данных" предназначена для настройки механизмов контроля целостности (КЦ) и замкнутой программной среды (ЗПС). В ходе настройки для механизма контроля целостности определяются списки контролируемых объектов, методы и расписание проведения контроля, реакция системы на результат контроля. Для замкнутой программной среды 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.

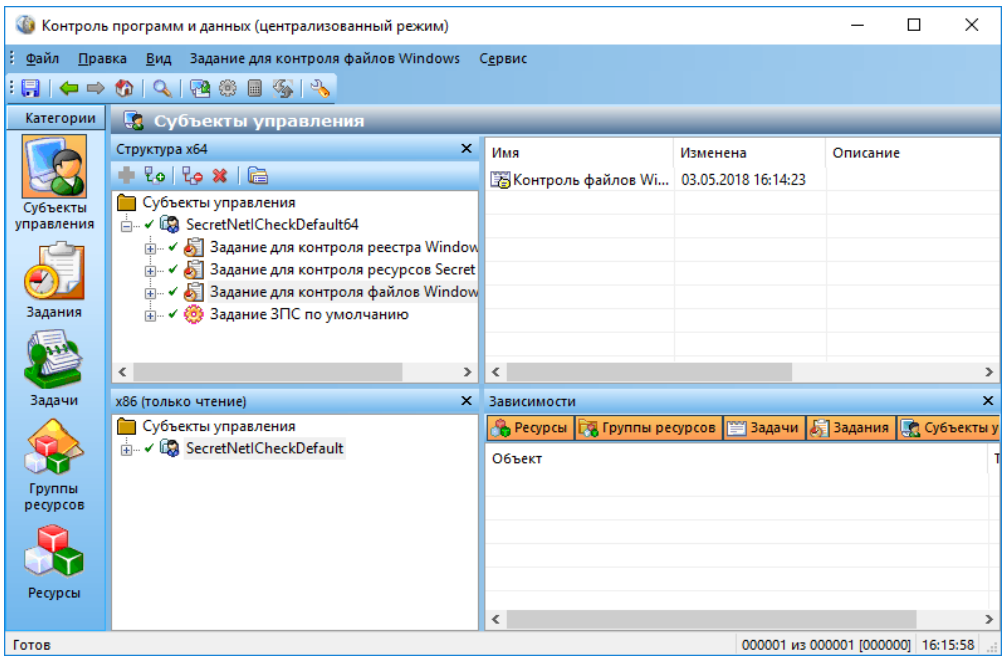
Для запуска программы в централизованном режиме:

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 программа 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.

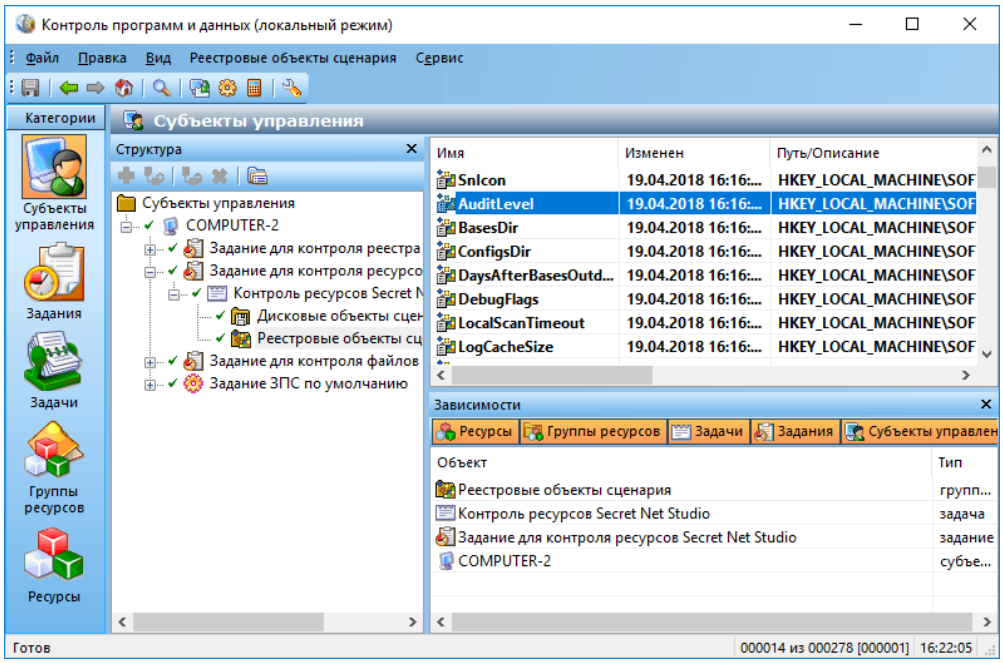
Пример содержимого окна программы в централизованном режиме представлен на следующем рисунке.



Для запуска программы в локальном режиме:

- в меню "Пуск" ОС Windows в группе "Код безопасности" выберите элемент "Контроль программ и данных (централизованный режим)".

Пример содержимого окна программы в локальном режиме представлен на следующем рисунке.



Глава 2
Настройка локальной аутентификации

Управление режимами механизма защиты входа в систему

Действие механизма защиты входа в систему регулируется рядом параметров, которые определяют работу соответствующих режимов механизма.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в программе управления (см. стр. 11). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для настройки режимов механизма защиты входа:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [4].

2. В разделе "Политики" перейдите к группе параметров "Вход в систему".
3. Настройте параметры, перечисленные ниже.

Максимальный период неактивности до блокировки экрана
Устанавливает максимально возможный период неактивности, после которого компьютер автоматически блокируется средствами системы Secret Net Studio. В целях безопасности при продолжительном бездействии пользователя компьютер должен блокироваться. Блокировка по истечении заданного периода неактивности осуществляется средствами системы Secret Net Studio. 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 Secret Net Studio не осуществляется
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)
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 Secret Net Studio (например eToken). **Блокировать станцию при изъятии любого идентификатора** — выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора любого типа из числа поддерживаемых системой Secret Net Studio для идентификации пользователей (iButton, eToken и др.). Блокировка при изъятии идентификатора применяется, если идентификатор активирован средствами Secret Net Studio и пользователь предъявил этот идентификатор для входа в систему

Количество неудачных попыток аутентификации
Устанавливает ограничение на количество неудачных попыток входа в систему при включенном режиме усиленной аутентификации по паролю. При достижении ограничения компьютер блокируется и вход разрешается только для администратора. Если установлено значение "0" — ограничение не действует
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
Режим идентификации пользователя
По имени. Для входа в систему пользователь должен ввести свои учетные данные, используя только стандартные средства ОС Windows. **Смешанный.** Для входа в систему пользователь может предъявить идентификатор, активированный средствами Secret Net Studio, или ввести свои учетные данные, используя стандартные средства ОС Windows. **Только по идентификатору.** Для входа в систему пользователь должен предъявить идентификатор, активированный средствами Secret Net Studio. Пользователи, не имеющие персональных идентификаторов, войти в систему не смогут. Администратор может войти в систему без предъявления идентификатора только в административном режиме (см. стр.**25**). В режимах входа "По имени" и "Смешанный" допускается работа с USB-ключами и смарт-картами средствами ОС Windows (см. документацию на ОС Windows). В режиме "Только по идентификатору" используются персональные идентификаторы, активированные средствами Secret Net Studio, но не ОС Windows
Режим аутентификации пользователя
Стандартная аутентификация — при входе пользователя выполняется только стандартная аутентификация ОС Windows. **Усиленная аутентификация по паролю** — при входе пользователя, помимо стандартной аутентификации ОС Windows, 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" в диалоге настройки свойств пользователя). 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
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". При необходимости могут применяться особые требования для паролей, сохраняемых в базе данных системы Secret Net Studio (независимо от заданных параметров политики паролей Windows). Для этого выберите режим "Задать свои значения" и настройте требования, аналогичные стандартным параметрам политики паролей Windows "Минимальная длина пароля", "Срок действия пароля" и "Сложность пароля". При этом на компьютерах в конечном итоге будут применяться наиболее "строгие" параметры из тех, которые заданы в политиках Secret Net Studio и Windows

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

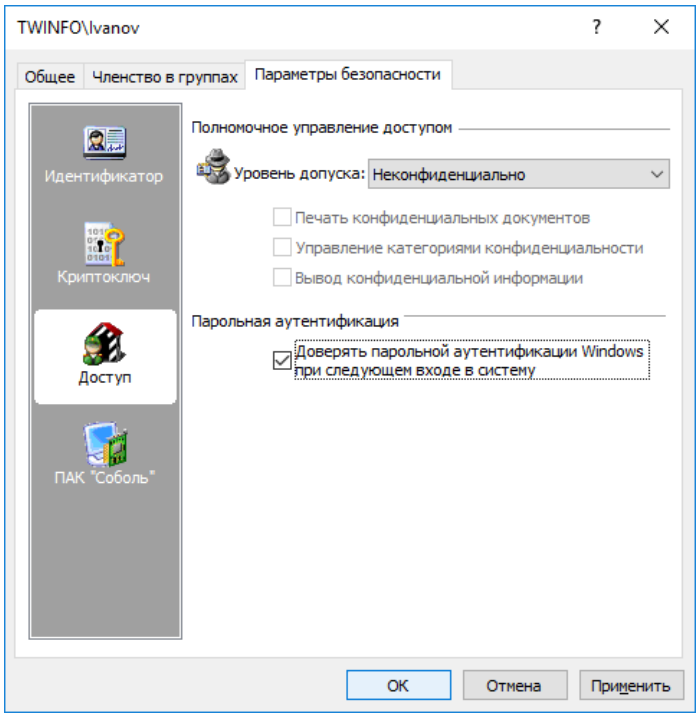
Если используется режим усиленной аутентификации пользователей по паролю, при входе пользователя дополнительно выполняется аутентификация по его паролю средствами Secret Net Studio. Для этого информация о пароле пользователя должна быть сохранена в базе данных Secret Net Studio. Сохранение этой информации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

В Secret Net Studio имеется 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.

Для разрешения разового входа пользователя в систему:

1. Запустите программу управления пользователями (см. стр.12).
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".

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. главу **4**);
- 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
Переход в сетевой режим	
Удаление системного журнала	Соболь: очистка журнала
Ошибка КС внешнего запроса	Соболь: ошибка синхронизации параметров
Ошибка внешнего запроса	
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	
Ошибка при контроле целостности	Соболь: нарушена целостность ресурса
Обработаны внешние запросы	Соболь: синхронизация параметров
Добавлен новый пользователь	
Пользователь удален	
Все пользователи удалены	
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

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.
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.**32**).

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 [**2**]);
   - сгенерируйте ключи централизованного управления комплексами "Соболь" (см. ниже);
   - подключите ПАК "Соболь" к Secret Net Studio (см. ниже);
   - 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". При установке для использования с клиентом в сетевом режиме функционирования выполните повторную регистрацию администратора с использованием идентификатора, подготовленного при выполнении действия **1** , и 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. Сведения об установке и настройке ПАК "Соболь" см. в документации на изделие;
   - установите ПО системы Secret Net Studio в сетевом режиме функционирования (см. документ [**2**]);
   - подключите ПАК "Соболь" к Secret Net Studio (см. ниже).
3. На компьютерах с установленным клиентом в автономном режиме функционирования — 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.**12**).

2. В меню "Сервис" выберите команду "Генерация ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".

3. Предъявите идентификатор (см. стр. 28), 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;
   - 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.**12**).
2. В меню "Сервис" выберите команду "Загрузка ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите носитель (см. стр.**28**), 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.**12**).
2. В меню "Сервис" выберите команду "Копирование ключей ЦУ ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите идентификатор (см. стр.**28**), содержащий копируемые ключи централизованного управления ПАК "Соболь".

   Произойдет 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.**12**).
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.

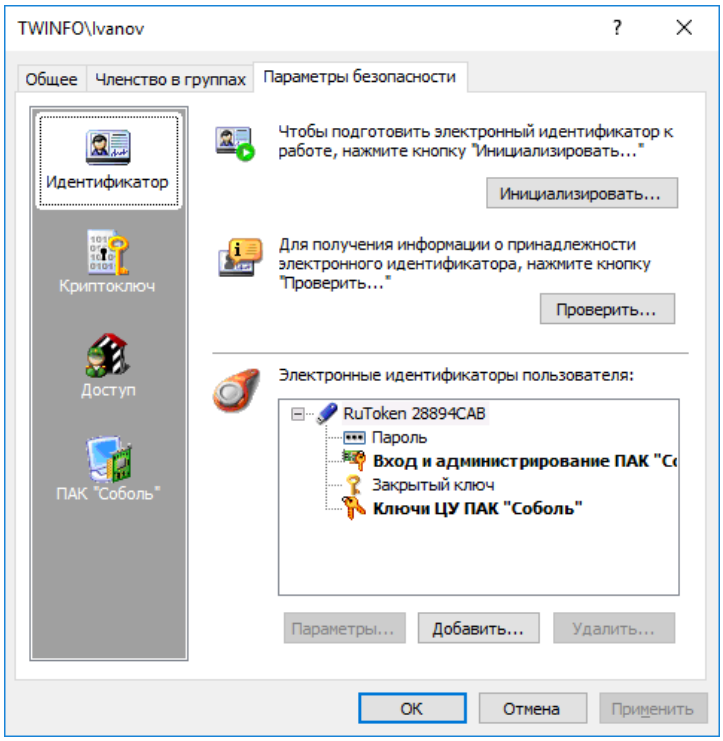
   На экране появится запрос на продолжение операции.

4. Нажмите кнопку "Да" в диалоге запроса.

   Произойдет удаление ключей из системы, после чего на экране появится запрос на удаление ключей из идентификаторов.

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.**22**).

Для копирования идентификатора администратора ПАК "Соболь":

1. Запустите программу управления пользователями (см. стр.**12**).
2. В меню "Сервис" выберите команду "Копирование идентификатора администратора ПАК "Соболь".

   На экране появится диалог "Предъявите идентификатор".

3. Предъявите идентификатор (см. стр.**28**) 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.

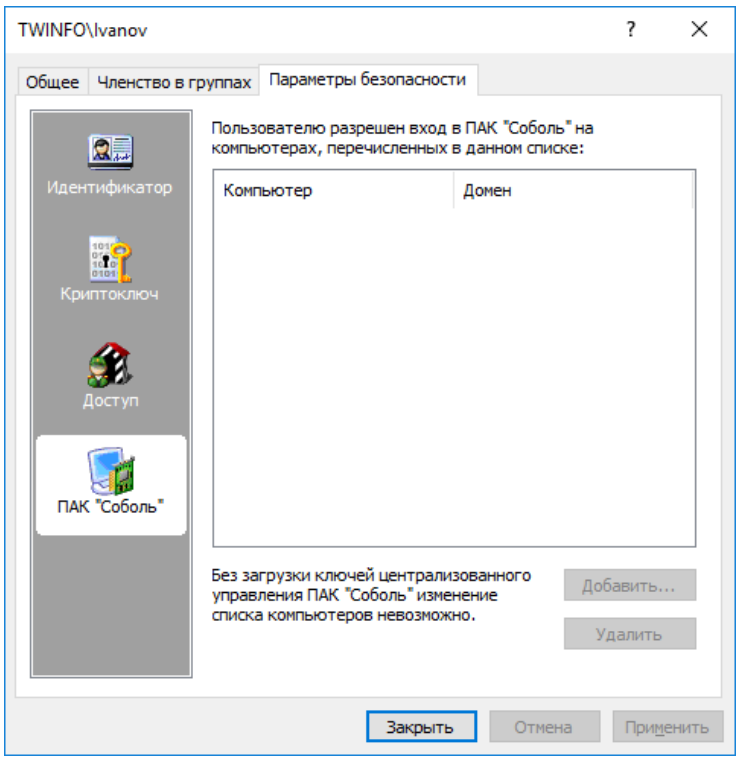
Чтобы предоставить такую возможность доменному пользователю, необходимо выполнить следующие действия:

- присвоить пользователю идентификатор с включенным режимом разрешения входа в ПАК "Соболь" (см. стр. **30**). Для идентификаторов, присвоенных пользователю ранее, включить режим можно при настройке режимов использования идентификатора (см. стр.**32**);
- 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.**22**).

Для формирования списка компьютеров:

1. В программе управления пользователями вызовите окно настройки свойств доменного пользователя и перейдите к диалогу "Параметры безопасности" (см. стр.**12**).
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.

Смена пароля пользователя администратором

Смена пароля пользователя может быть выполнена самим пользователем или администратором. Описание смены пароля пользователем см. в документе [**9**].

Внимание!

- Для клиентов в сетевом режиме функционирования при включенном режиме усиленной аутентификации по паролю (см. стр.16) 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. стр.7). 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.**12**).
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 и нажмите кнопку "OK".

   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.**28**).

   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".

Вход в систему в административном режиме

При штатном функционировании системы Secret Net Studio вход любого пользователя компьютера, включая администратора, должен выполняться по одинаковым правилам, установленным соответствующими механизмами защиты. Во время загрузки компьютера перед входом пользователя система защиты проводит инициализацию защитных подсистем и их функциональный контроль. После успешного проведения всех проверок вход в систему разрешается.

В тех случаях, когда необходимо получить доступ к компьютеру в обход действующих механизмов или прервать выполнение инициализации подсистем, администратор может активировать 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.

Глава 3
Настройка аппаратной поддержки

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 или идентификаторы iButton.

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 необходимо 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

Причина	Действие
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.**12**).
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.**12**).
2. В меню "Сервис" выберите команду "Проверка идентификатора".

   На экране появится диалог "Предъявите идентификатор".
3. Предъявите проверяемый идентификатор (см. стр.**28**).

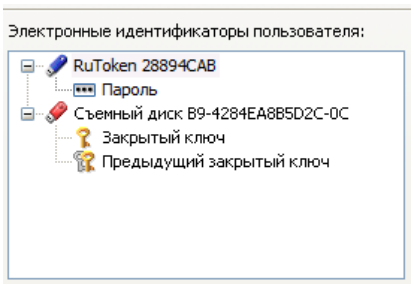
   Если в базе данных Secret Net Studio есть сведения об этом идентификаторе, они будут выведены на экран.

Работа с идентификаторами пользователей

Просмотр сведений об идентификаторах пользователя

Сведения о персональных идентификаторах пользователя представлены в программе управления пользователями (см. стр.**12**). 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

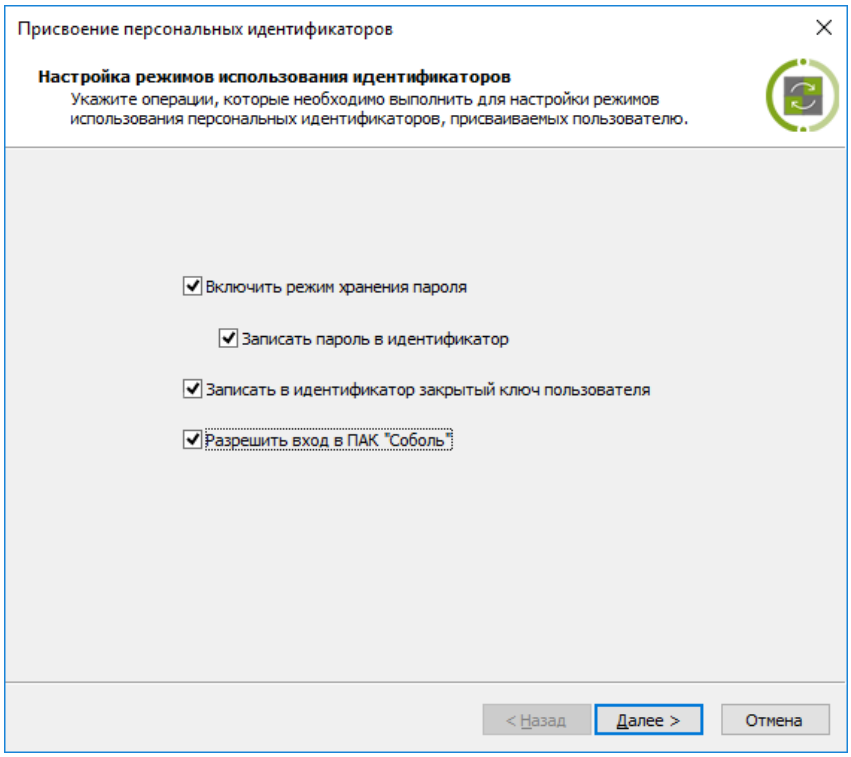
Процедура присвоения идентификатора пользователю выполняется с помощью программы-мастера. При присвоении можно настроить режимы использования персонального идентификатора.

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. 19).

Для присвоения идентификатора пользователю:

1. Запустите программу управления пользователями (см. стр. 12).
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.28), содержащий его закрытый ключ.

Успешно выполненные операции имеют статус "Выполнено". Если при выполнении операции произошла ошибка, в диалоге будет приведено соответствующее сообщение об этом.

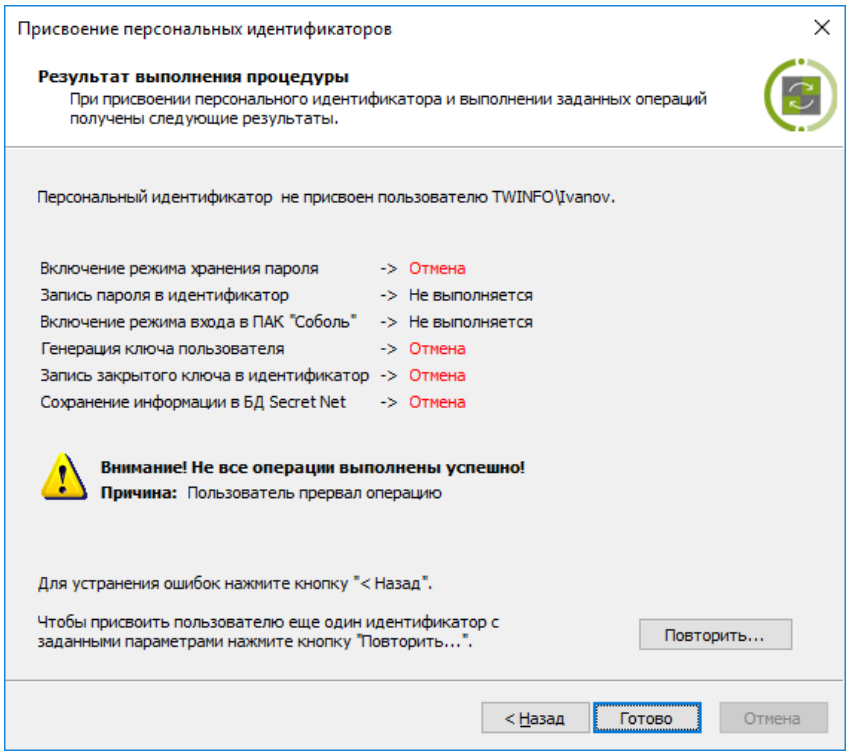
5. После успешного выполнения всех операций нажмите кнопку "Далее >".

   На экране появится диалог "Предъявите идентификатор".

6. Предъявите идентификатор (см. стр.28) 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 осуществляется, 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.

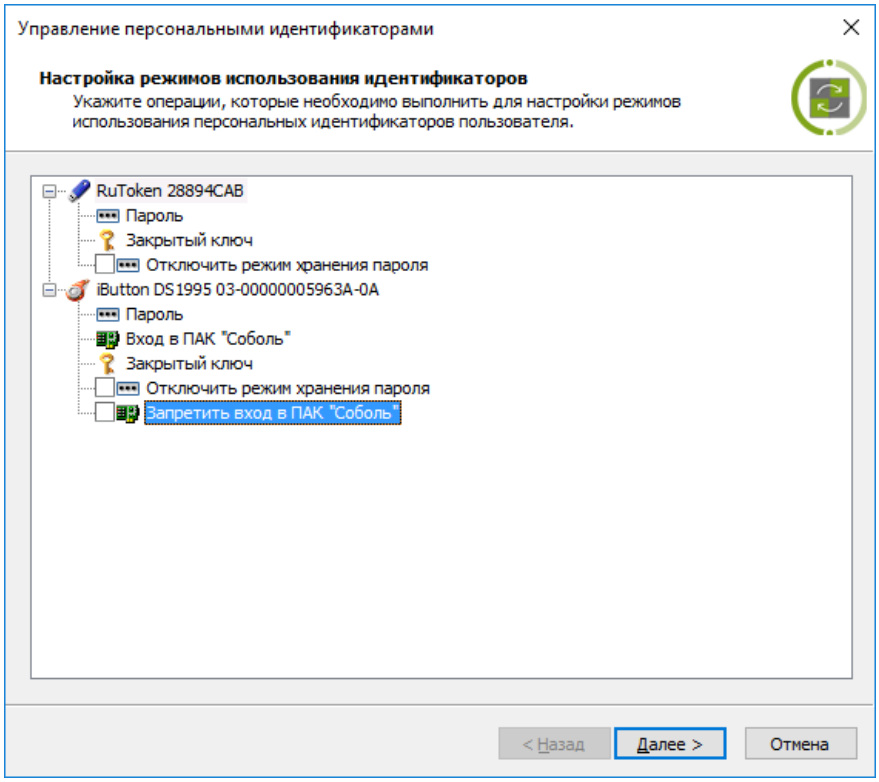
Настройка режимов использования идентификаторов

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.12).
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".

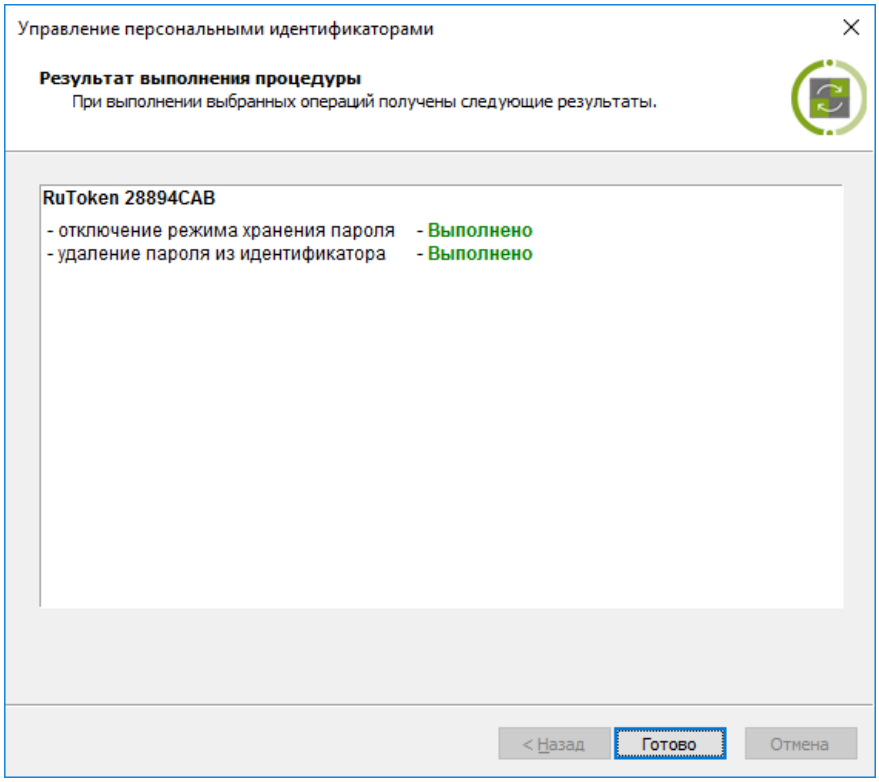
3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".
4. Если выбрана операция "Записать пароль в идентификатор" или "Разрешить вход в ПАК "Соболь", на экране появится диалог "Ввод пароля". Введите пароль пользователя и нажмите кнопку "ОК".

   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.**28**).

   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.**12**).
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.**28**).

   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 4
Настройка контроля целостности ресурсов

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

В системе Secret Net Studio настройка механизма КЦ может осуществляться совместно с настройкой механизма замкнутой программной среды (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. Описание настройки механизма замкнутой программной среды см. в документе [**5**].

Общие сведения о методах и средствах настройки

Модель данных

Состав

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

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	Задача — это 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
Субъект управления	Субъектом управления может быть 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 замкнутой программной среды

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 замкнутой программной среде, другая — к контролю целостности. 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

Локальная база данных (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 центральная база данных (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 отличаются 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

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 версией ОС

соответствующей разрядности и установленным клиентским ПО системы 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 процедур запуска программы см. на стр.**13**.

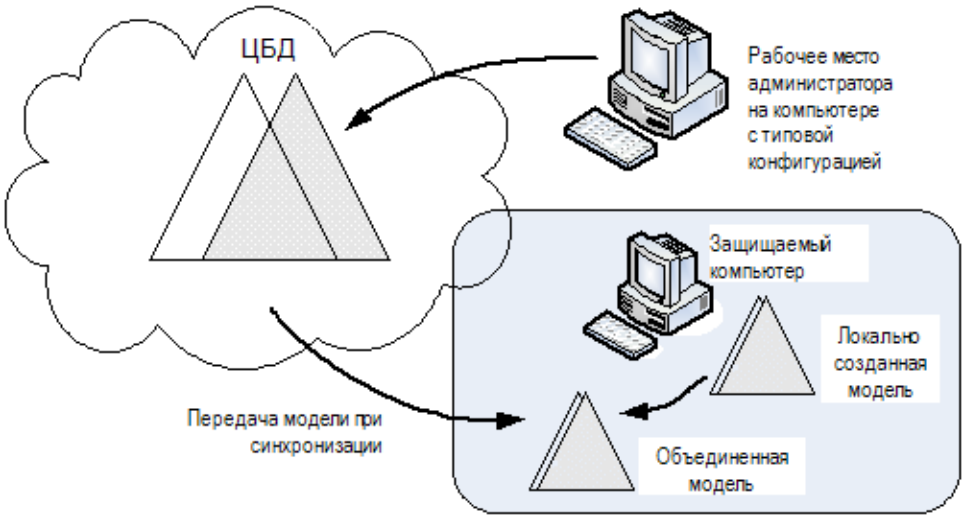
Синхронизация центральной и локальной баз данных

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. **51**). Для оперативной синхронизации на компьютерах должны быть настроены определенные параметры ОС Windows (см. стр.**101**).

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 механизма

В этом разделе рассматривается порядок начальной настройки механизма КЦ. 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 механизма КЦ выполните настройку в следующем порядке:

1. Сформируйте новую модель данных с настройкой контроля по умолчанию (см. стр.**39**).
2. Добавьте в модель данных дополнительные объекты:
   - задачи для контроля целостности (см. стр.**40**);
   - задания КЦ и ПАК "Соболь" (см. стр.**42**).
3. Создайте эталоны контролируемых ресурсов (см. стр.**46**).
4. Включите действие механизма КЦ (см. стр.**49**). Перед началом эксплуатации механизма рекомендуется выполнить проверку корректности параметров заданий контроля (см. стр.**49**).

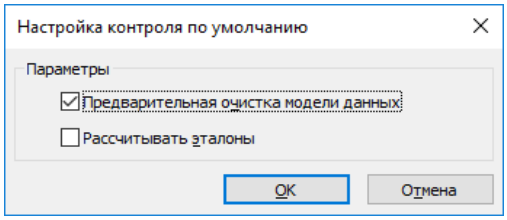
В процессе эксплуатации системы может возникнуть необходимость корректировки или пересмотра модели данных. Если предполагается кардинальная переработка модели, то лучше выполнить ее с нуля. Если переработке будет подвергнута небольшая часть модели, то в этом случае можно применить отдельные процедуры модификации модели (см. стр.**58**).

Формирование новой модели данных

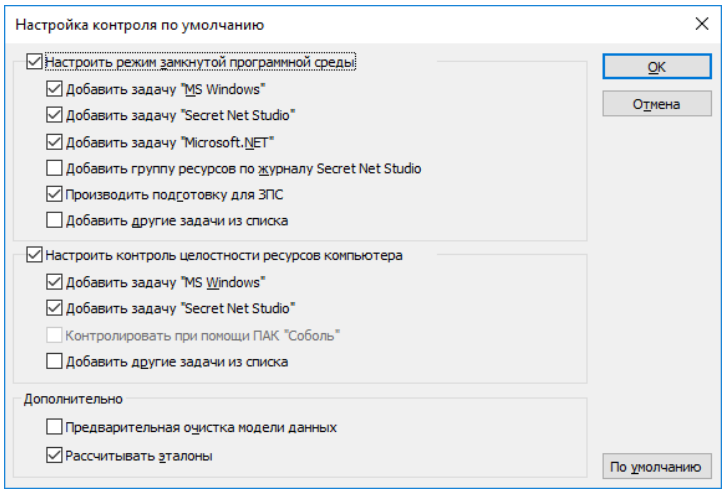
При формировании в модель данных автоматически добавляются описания для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ. Новая модель данных будет сформирована с настройкой контроля по умолчанию.

Для формирования новой модели данных:

1. В программе управления 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

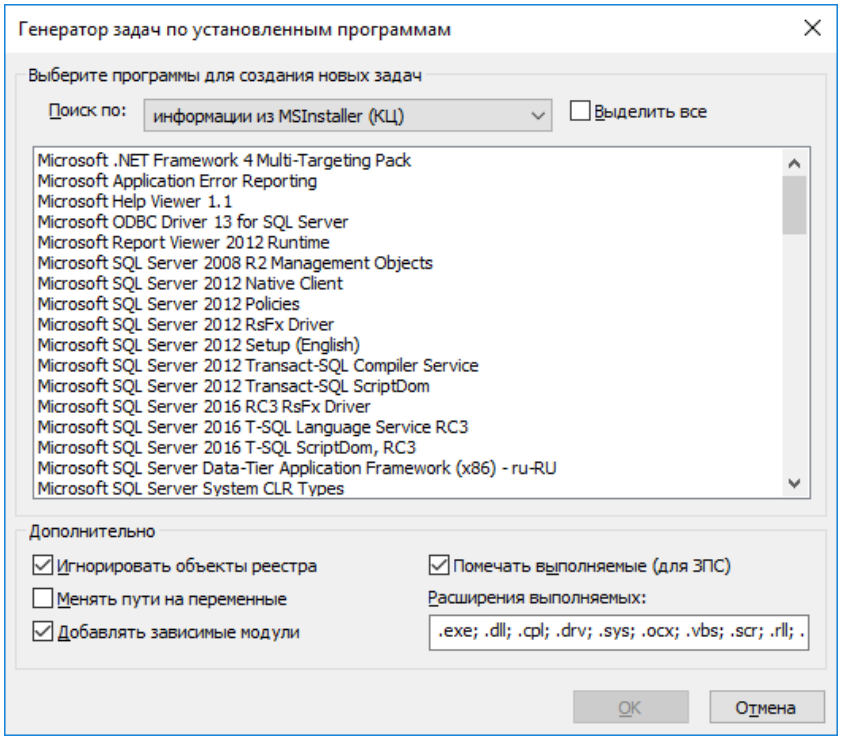
Целью данного этапа настройки является дополнение модели данных фрагментом, включающим список других необходимых задач (помимо ресурсов Windows и Secret Net Studio). Для этого могут быть использованы как ручные методы, так и специальное средство — механизм генерации задач. Задачи создаются на основании 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.

Для добавления в модель задач с помощью механизма генерации:

1. Выберите в меню "Сервис" 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
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.95). 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 "OK".

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

5. Нажмите кнопку "OK" 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 контроля целостности 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.

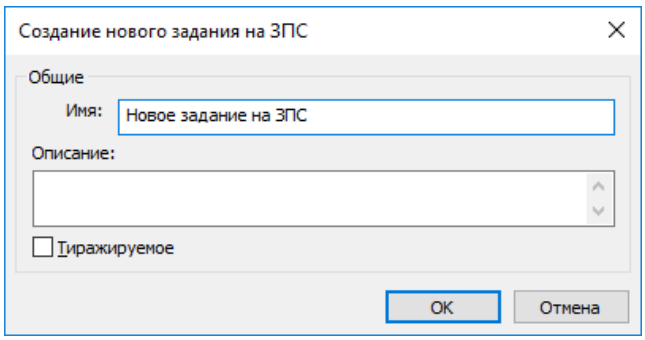
Для формирования задания:

1. Выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание".

   На экране появится диалог выбора типа задания.

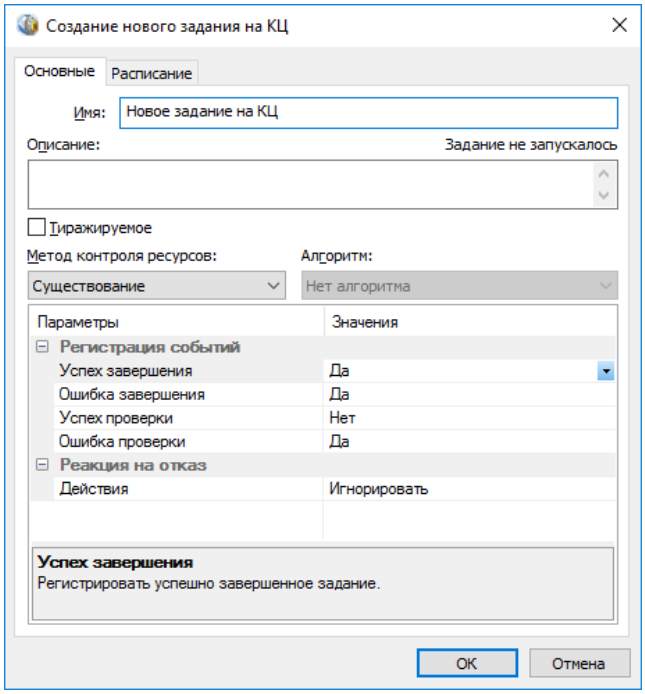
2. Выберите тип задания (КЦ или ПАК "Соболь") и нажмите кнопку "OK".

   Если выбрано задание ЗПС или ПАК "Соболь", на экране появится диалог:



   Введите имя задания, его краткое описание и нажмите кнопку "OK". Порядок настройки задания для ПАК "Соболь" описан на стр.**76**.

   Если выбрано задание КЦ, на экране появится диалог.



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

   Предусмотренные методы перечислены в следующей таблице.

Метод контроля	Что проверяется
Существование	Наличие ресурсов по заданному пути
Содержимое	Целостность содержимого ресурсов
Атрибуты	Стандартные атрибуты, установленные для ресурсов
Права доступа	Категории конфиденциальности и атрибуты доступа Windows (дескриптор безопасности), установленные для ресурсов

При выборе типа контролируемых данных необходимо иметь в виду, что проверка будет выполняться только для определенных типов ресурсов. Сведения о применимости методов контроля для каждого из типов ресурсов в зависимости от выбранного типа контролируемых данных приведены ниже. При выборе метода контроля может оказаться, что с заданием связаны ресурсы, несовместимые с используемым в задании алгоритмом. Это довольно типичная ситуация, когда на контроль ставится комплексная задача, состоящая из большого количества разнородных ресурсов. Такой ситуации не следует опасаться — несовместимые ресурсы подсистемой контроля игнорируются. При расчете эталонов желательно на несовместимые ресурсы использовать реакции "игнорировать" или "выводить запрос". Таким образом, можно связывать с задачей сразу несколько разных заданий на контроль, не беспокоясь, что наличие несовместимых с заданиями ресурсов вызовет сбои.

Соответствие типов ресурсов и методов контроля представлено в следующей таблице.

	Содержимое объекта	Атрибуты объекта	Права доступа	Существование объекта
Файл	Да	Да	Да	Да
Каталог	Да	Да	Да	Да

	Содержимое объекта	Атрибуты объекта	Права доступа	Существование объекта
Ключ реестра	Да	Нет	Да	Да
Значение реестра	Да	Нет	Нет	Да

5. Если указан метод контроля "Содержимое", укажите алгоритм, выбрав его из списка.

   Предусмотрены следующие алгоритмы: CRC32, ЭЦП, хэш, имитовставка, полное совпадение, встроенная ЭЦП.

   Особенности некоторых алгоритмов

   Алгоритм "полное совпадение", в отличие от других, предусматривает возможность восстановления контролируемого объекта в случае нарушения его целостности. Однако при использовании данного алгоритма существенно увеличивается объем базы данных — поскольку эталонным значением для контроля является копия объекта.

   Алгоритм "встроенная ЭЦП" позволяет обеспечить выполнение контроля целостности файлов, обновленных при установке обновлений ПО приложений и операционной системы. Алгоритм отличается тем, что при контроле целостности осуществляется проверка встроенной цифровой подписи файлов (формат подписи Microsoft Authenticode). Необходимым условием для успешного завершения проверки является неизменность сертификата подписанного файла. Если при расчете эталонов для файла не обнаружена встроенная цифровая подпись, этот файл будет игнорироваться при контроле с использованием данного алгоритма.

6. Настройте регистрацию событий. Для этого в столбце "Параметры" выберите нужное событие. В соответствующей строке столбца "Значения" появится значок раскрывающегося списка. Выберите в списке значение "Да", чтобы данное событие регистрировалось, или "Нет", чтобы регистрация не осуществлялась.

   Предусмотренные события перечислены в следующей таблице.

Событие	Описание события
Успех завершения	Успешное завершение задания на контроль целостности
Ошибка завершения	Обнаружено нарушение целостности при обработке задания
Успех проверки	Успешная проверка целостности ресурса
Ошибка проверки	Нарушение целостности ресурса

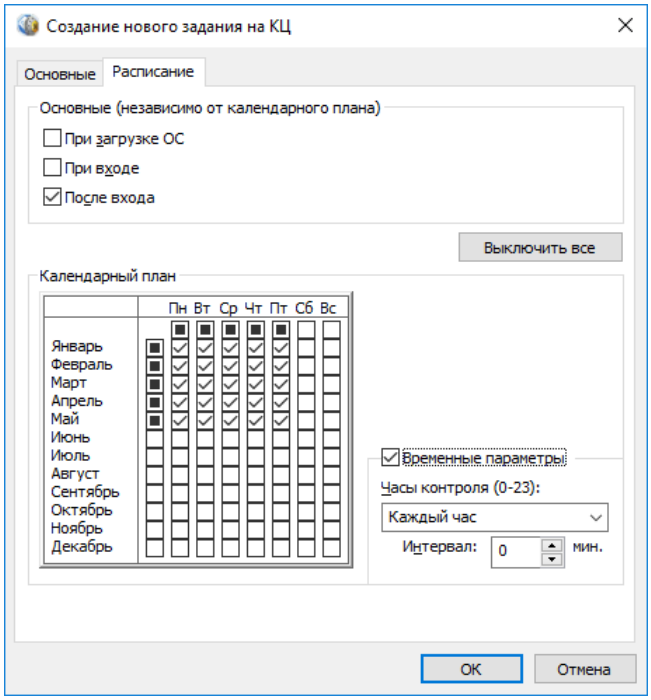
7. Настройте реакцию системы. Для этого выделите в столбце "Параметры" строку "Действие", а в столбце "Значения" выберите нужный вариант. Предусмотрены следующие варианты:

Реакция	Пояснение
Игнорировать	Реакция системы отсутствует
Заблокировать компьютер	Компьютер блокируется. Снять блокировку может только администратор безопасности
Восстановить из эталона	Текущее значение контролируемого параметра ресурса восстанавливается из эталона. Реакция доступна не для всех методов
Восстановить с блокировкой	Текущее значение контролируемого параметра ресурса восстанавливается из эталона. Компьютер блокируется. Снять блокировку может только администратор безопасности. Реакция доступна не для всех методов
Принять как эталон	Текущее значение контролируемого параметра ресурса принимается за эталон. Эта реакция недоступна для тиражируемых заданий

Для файлов и значений реестра возможность восстановления имеет следующие особенности:

- восстановление не предусмотрено, если используется метод контроля "Существование";
- восстановление возможно, если используется метод контроля "Содержимое" и в нем применяется алгоритм "Полное совпадение";
- могут быть восстановлены атрибуты файлов и каталогов, если используется метод контроля "Атрибуты" (кроме меток конфиденциальности системы Secret Net Studio).

8. Перейдите к диалогу "Расписание" и составьте расписание контроля в соответствии с требованиями к заданию.



Диалог разделен на две части. В верхней части настраивается время проведения проверки независимо от календаря (при загрузке операционной системы, при входе пользователя в систему и после входа в систему). В нижней части расположены календарь и средства настройки расписания в течение суток.

Поле	Использование
Основные (независимо от календарного плана)	С помощью полей этой группы можно указать, на каком этапе своей работы система защиты должна контролировать целостность ресурсов. Проверка может проводиться при загрузке операционной системы, при входе пользователя в систему и после входа в систему. В режиме "При входе" проверка начинается после ввода пользователем идентификационных признаков, и до завершения проверки процесс входа в систему приостанавливается. Если установлен режим "После входа" — проверка начнется после входа пользователя в систему и продолжается в фоновом режиме
Календарный план	Группа полей для включения контроля по месяцам, дням недели, часам и минутам
Календарь	С помощью календаря можно указать расписание контроля по месяцам и дням недели
Временные параметры	С помощью полей этой группы можно указать периодичность контроля в течение суток

Поле	Использование
Часы контроля	Введите или выберите из раскрывающегося списка значение периодичности контроля в течение суток. Можно выбрать период, а можно и непосредственно ввести конкретные значения. Следует иметь в виду, что отсчет начинается с нулевого часа. Поэтому если вы установите значение 4, что означает – "проводить контроль каждый четвертый час", контроль будет проводиться в 0, 3, 7, 11 и т. д. Часы контроля можно задать, не только указав периодичность, но и непосредственно введя конкретные значения. Например, если вы введете следующую строку: 2, 7–9, 16–18, 21, то контроль будет проведен в 2, 7, 8, 9, 16, 17, 18 и 21 час
Интервал	Укажите периодичность контроля в течение часа контроля. Если значение не указано, контроль выполняется в начале часа один раз. Так, например, если контроль должен проводиться в 7 часов, а в поле "Интервал" указано значение 10, то процесс контроля первый раз начнется в 7 часов 00 минут, а затем будет повторяться каждые 10 минут в течение этого часа

9. Нажмите кнопку "OK".

   В дополнительном окне структуры появится новое задание контроля целостности, не связанное с субъектами. Тиражируемое задание обозначается пиктограммой .

Внимание!
Задания, созданные средствами централизованного управления, отображаются в программе, работающей в локальном режиме, жирным 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".

Расчет эталонов

Расчет эталонов необходим для контролируемых ресурсов, входящих в задания контроля целостности, 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.39). 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 "Контроль программ и данных" 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,

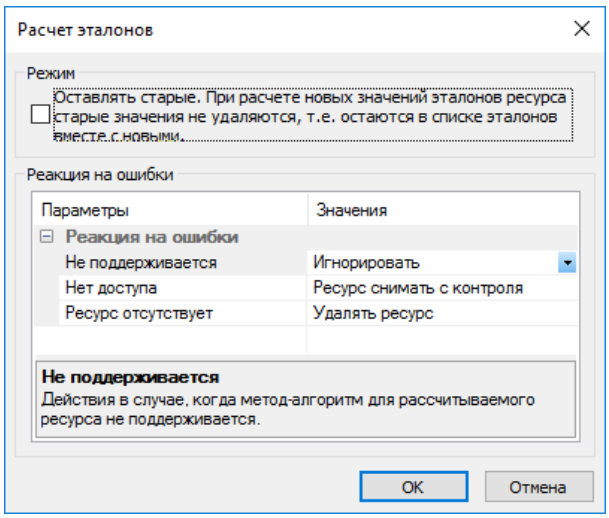
эталоны которых рассчитаны централизованно (ресурсы входят в тиражируемые задания).

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. 73.

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 следующей таблице.

Реакция	Описание
Игнорировать	Реакция системы на ошибку отсутствует

Реакция	Описание
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".

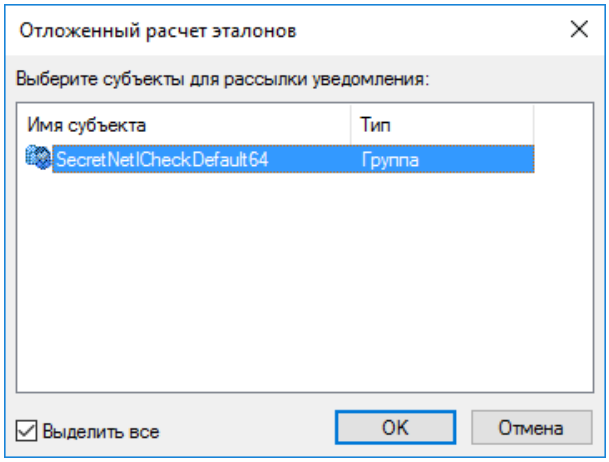
   На экране появится диалог "Расчет эталонов".

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 установке 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.

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.**54**, стр.**56**).

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. **95**). 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.

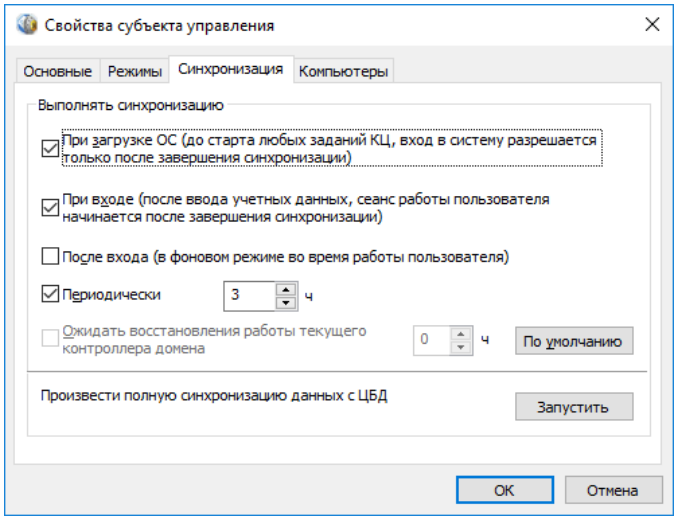
Настройка параметров запуска синхронизации осуществляется в централизованном режиме работы программы. Параметры могут быть заданы как для отдельных компьютеров, так и для групп. При этом действуют приоритеты применения параметров: наивысший приоритет имеют параметры компьютеров, затем параметры групп, 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 "OK".

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".

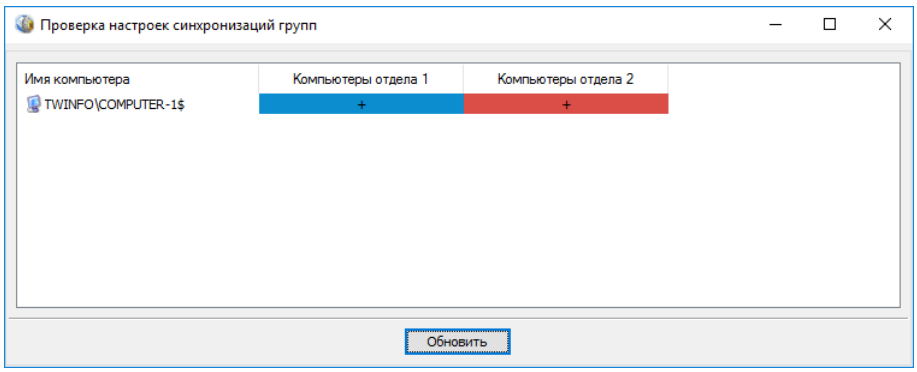
   Примечание.
   Команда недоступна, если список субъектов в модели данных содержит только одну группу по умолчанию SecretNetICheckDefault.

   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.**51**). При работе с программой 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 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

Процедура экспортирования может осуществляться следующими способами:

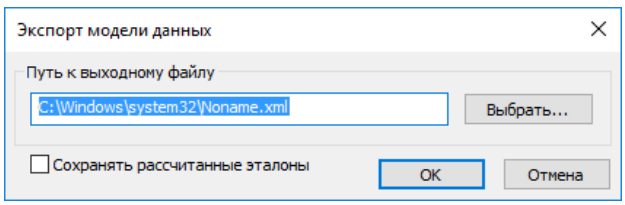
- экспортирование всей модели данных;
- выборочное экспортирование объектов определенных категорий (не применяется к объектам категории "Субъекты управления").

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.103.

Для экспортирования текущей модели данных:

1. В меню "Файл" выберите команду "Экспорт модели в XML".

   На экране появится диалог настройки параметров экспортирования.



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 экспортирования 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 экспортирования.

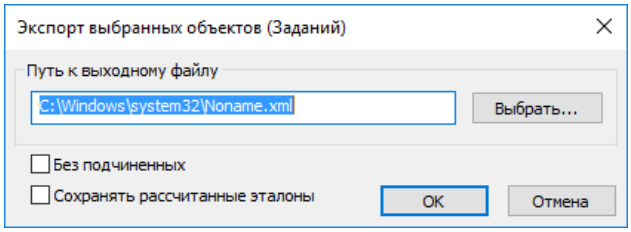
Для выборочного экспортирования объектов:

1. На панели категорий выберите категорию, в которой содержатся нужные объекты для экспортирования (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 экспортирования. 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 экспортирования.



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 экспортирование осуществляется для 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 экспортирования 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 экспортирования.

Импорт

Процедура импорта из файла может выполняться следующими способами:

- общее импортирование объектов в модель данных — позволяет импортировать все данные, хранящиеся в файле;
- импортирование объектов в текущую категорию (не применяется к категории "Субъекты управления") — позволяет импортировать из файла объекты, относящиеся к той же категории.

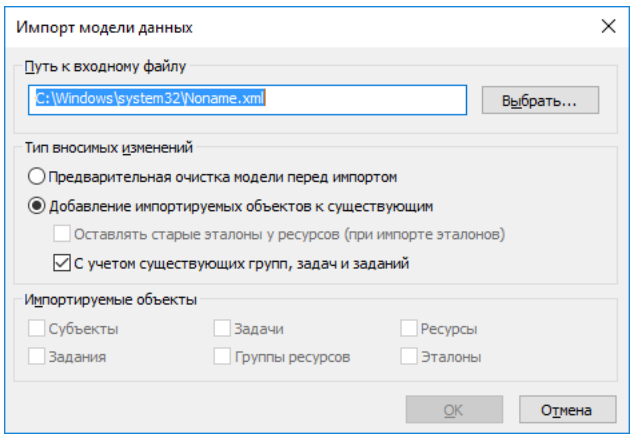
Импортом из файла с сохраненной моделью данных добавляются списки ресурсов, экспортированные из другой модели данных. Данный способ используется при переносе настроек защитных механизмов с одного компьютера на другой. Компьютеры должны иметь сходные конфигурации и использовать одинаковое программное 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 импортирования 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 импортирования.



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 импортирования. 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

Поле	Пояснение
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 импортирования 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".

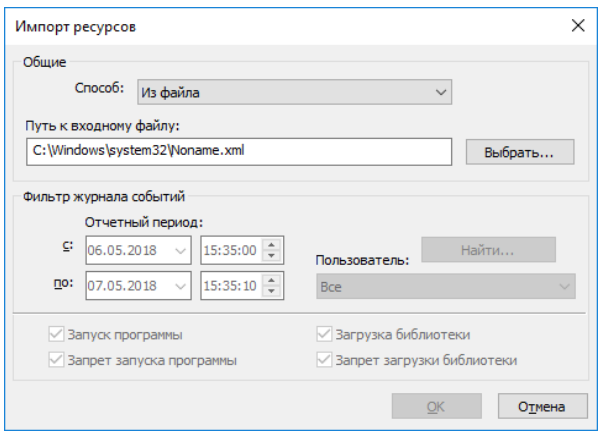
7. Нажмите кнопку "OK" в диалоге настройки параметров импортирования.

Для импортирования объектов текущей категории:

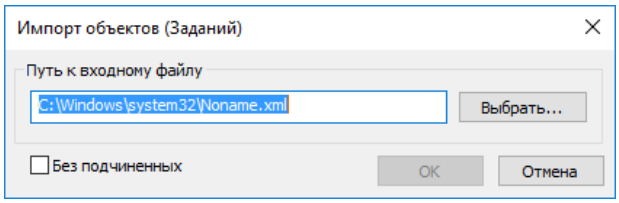
1. На панели категорий выберите категорию, в которую нужно импортировать объекты (кроме категории "Субъекты управления").
2. В окне структуры выберите корневой элемент. Откройте меню с названием элемента (например, "Задание") и выберите команду "Импорт и добавление".

   На экране появится диалог настройки параметров импортирования.

   - 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 "ОК".

   Объекты, хранящиеся в файле, будут добавлены в список объектов текущей категории. При импортировании 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 импортирования 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.
Избирательное импортирование эталонных значений ресурсов не осуществляется. Если требуется импортировать эталонные значения, выполните процедуру общего импортирования 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:

Группа операций	Ссылка
Изменение параметров объектов	стр.**59**
Изменение параметров ресурса	стр.**59**
Изменение параметров группы ресурсов	стр.**59**
Изменение параметров задачи	стр.**59**
Изменение параметров задания	стр.**59**
Просмотр параметров субъекта управления	стр.**59**

Группа операций	Ссылка
Добавление объектов	стр.**63**
Добавление вручную одиночного ресурса	стр.**63**
Добавление вручную нескольких ресурсов	стр.**63**
Импорт списка ресурсов из журнала безопасности ОС Windows	стр.**63**
Импорт списка ресурсов из журнала Secret Net Studio	стр.**63**
Добавление ресурса в группу	стр.**63**
Добавление группы ресурсов вручную	стр.**63**
Добавление группы ресурсов по каталогу	стр.**63**
Добавление группы ресурсов по ключу реестра	стр.**63**
Добавление группы ресурсов средствами импорта	стр.**63**
Добавление задачи вручную	стр.**63**
Добавление задачи с помощью генератора задач	стр.**40**
Добавление задачи с помощью средств импорта	стр.**56**
Добавление заданий	стр.**42**
Добавление субъектов	стр.**49**
Удаление объектов	стр.**72**
Удаление объекта	стр.**72**
Удаление всех объектов определенной категории	стр.**72**
Связывание объектов	стр.**73**
Связывание объектов	стр.**73**
Удаление связи между объектами	стр.**73**
Новый расчет и замена эталонов	стр.**73**
Поиск зависимых модулей	стр.**74**
Замена переменных окружения	стр.**75**
Настройка задания для ПАК "Соболь"	стр.**76**

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.**75**).

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 контроля целостности, 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 — см. стр. **95**) 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 CS6 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.**69**).
3. Внесите изменения в поля "Имя" и "Описание" и нажмите кнопку "ОК".

Параметры задания

Свойства задания контроля целостности 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 контроля целостности 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) контроля целостности. 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".

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 "ОК". Действия выполняются аналогично процедуре формирования задания (см. стр.**42**).

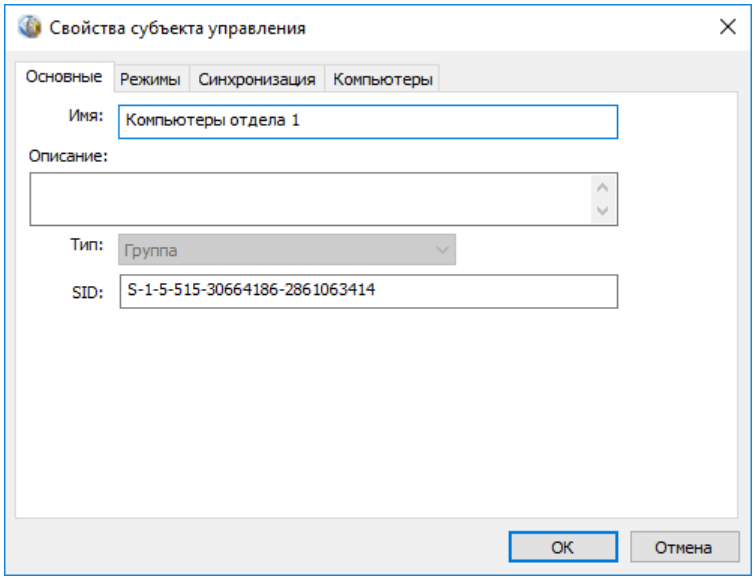
Параметры субъектов

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 следующем 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 "OK".

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.**56**); • 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

Параметр	Пояснение
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:

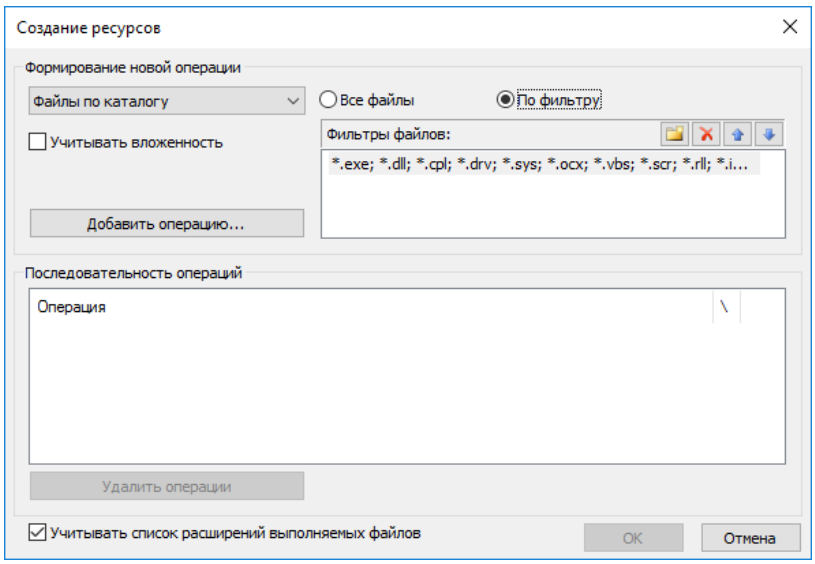
Параметр	Пояснение
Имя	Введите имя ресурса, уникальное для списка ресурсов. В качестве имени ресурса можно указать, например, имя файла, из которого загружен сценарий (скрипт)
Описание	Введите дополнительные сведения о ресурсе
Содержимое	Введите текст сценария (скрипта) — последовательность исполняемых 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.**95**). 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.

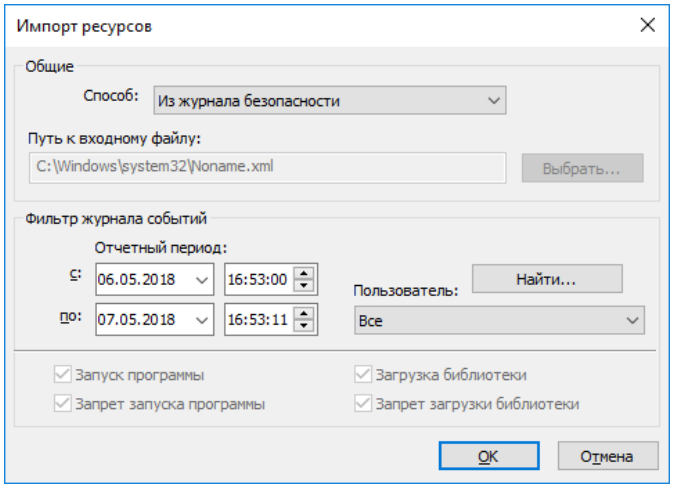
9. Проверьте список выполненных операций и, если он содержит все ресурсы, которые планировалось включить в модель данных, нажмите кнопку "ОК".

   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 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 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.**57**), 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 импортирования.
3. Выполните действия для импортирования объектов категории (описание процедуры импортирования см. на стр.**56**).

Добавление задач

Добавить новую задачу в модель данных можно одним из следующих способов:

- вручную;
- вручную со сценарием;
- с помощью генератора задач (см. стр.**40**);
- с помощью средств импорта (см. стр.**56**).

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".

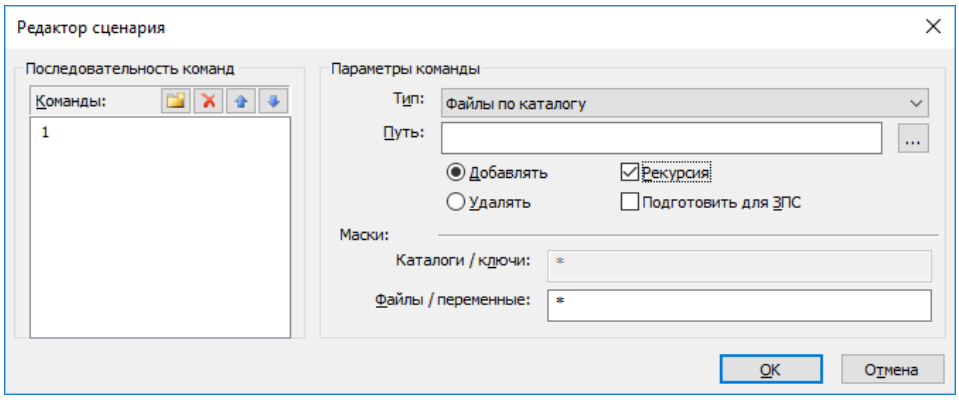
   В модели данных появится новая задача, не связанная с другими объектами.

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.74). 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.**42**.

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".

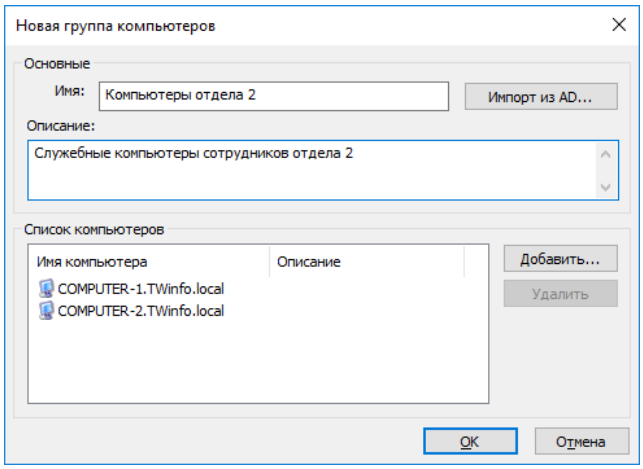
   Появится диалог со списком компьютеров домена безопасности с установленным клиентским ПО Secret Net Studio.
4. Выберите в списке нужные компьютеры и нажмите кнопку "ОК".

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 (объекты) 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 импортировании 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.**46**). 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 контроля целостности. 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.**59**).
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.**46**).

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

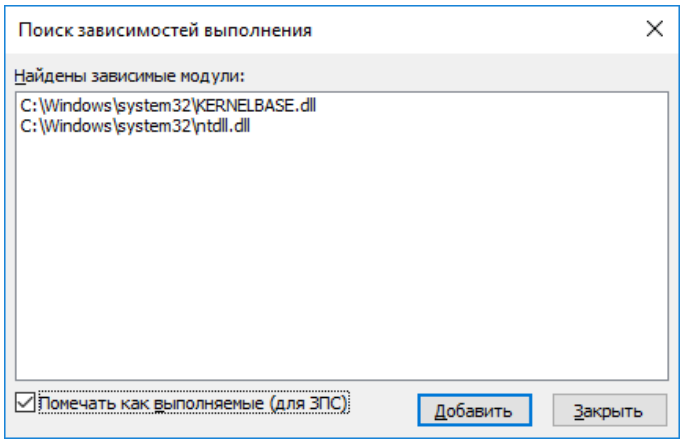
При работе пользователя с приложениями запуск исполняемых файлов может сопровождаться запуском модулей (драйверов и библиотек), не входящих непосредственно в приложения. Такие модули называются зависимыми.

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 экспортирование 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. Задание на контроль целостности физических секторов формируется средствами комплекса "Соболь". Задание на контроль целостности файлов и объектов реестра формируется либо средствами комплекса "Соболь", либо средствами программы "Контроль программ и данных" из состава ПО системы Secret Net Studio.
Рекомендуется задание на контроль целостности файлов и объектов реестра формировать средствами программы "Контроль программ и данных".

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, 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 5
Настройка аудита

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 программе управления (см. стр. 11). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для настройки параметров журнала:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [4].

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. К таким событиям, например, относятся события категории "Регистрация". Отключить регистрацию таких событий нельзя.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в программе управления (см. стр. 11). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для настройки списка регистрируемых событий:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [4].

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".

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 программе управления (см. стр. 11). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для настройки параметров хранилища:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [4].

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 в хранилище 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 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. в документе [**5**].

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 программе управления.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в программе управления (см. стр. **11**). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для настройки контроля приложений:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [**4**].

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".

Предоставление прав доступа к журналам

Доступ к записям журналов предоставляется сотрудникам, ответственным за управление системой защиты. Права на загрузку записей и управление содержимым журналов определяются привилегиями пользователей:

- привилегии для работы с локальными журналами;
- привилегии для работы с централизованными журналами.

Привилегии для работы с локальными журналами

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.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в программе управления (см. стр. **11**). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для предоставления привилегий:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [**4**].

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".

Привилегии для работы с централизованными журналами

Для загрузки записей централизованных журналов используется программа управления. Описание предусмотренных привилегий для работы с программой см. в документе [**4**].

Глава 6
Локальный аудит

Общие сведения о регистрации событий на рабочей станции

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 программа управления в локальном режиме.

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).

Программа управления при работе в локальном режиме 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.

Хранилище теневого копирования

В хранилище теневого копирования помещаются дубликаты (копии) данных, выводимых на съемные 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 программе управления в локальном режиме работы 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 оно 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, с помощью 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, для этого 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.

Хранение и очистка локальных журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы (штатные журналы ОС Windows и журнал Secret Net Studio) и хранятся на компьютере локально. Пока записи хранятся в локальном хранилище, их можно загрузить в программу управления в локальном режиме 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 программе управления пользователь может выполнять экспорт записей журналов в файлы. Если пользователю предоставлена соответствующая привилегия, он может выполнять и очистку журналов.

Локальная работа с журналами

Для локальной работы с журналами может использоваться программа управления в локальном режиме (см. стр. 11). Процедуры загрузки и управления записями локальных журналов и журналов, сохраненных в файлах, выполняются аналогично, как при работе программы в централизованном режиме. Сведения о работе с программой управления в централизованном режиме приведены в документе [**4**]. Ниже рассматриваются возможности, доступные только при работе с программой в локальном режиме.

Экспорт записей локальных журналов

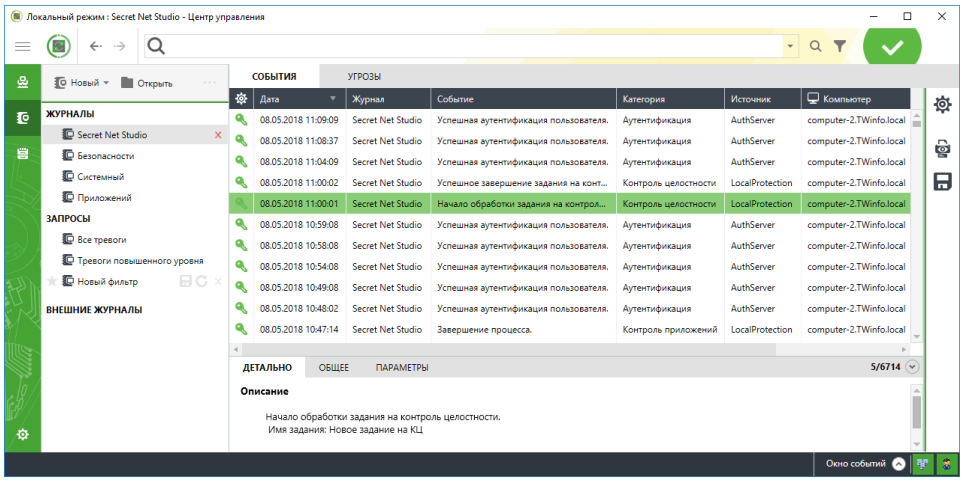
Программа управления в локальном режиме позволяет экспортировать (сохранять) в файлы записи локальных журналов. При экспорте предоставляется возможность очистки содержимого журнала после сохранения записей. Поддерживаемые форматы сохранения перечислены в следующей таблице.

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

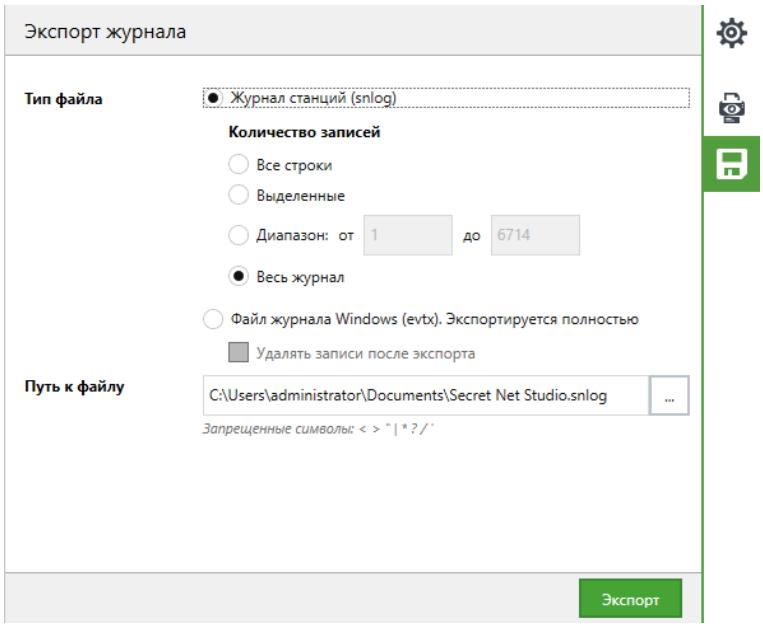
   Пример окна программы управления в локальном режиме с загруженными записями журнала Secret Net Studio представлен на следующем рисунке.



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.**80**)

7. Нажмите кнопку "Экспорт".

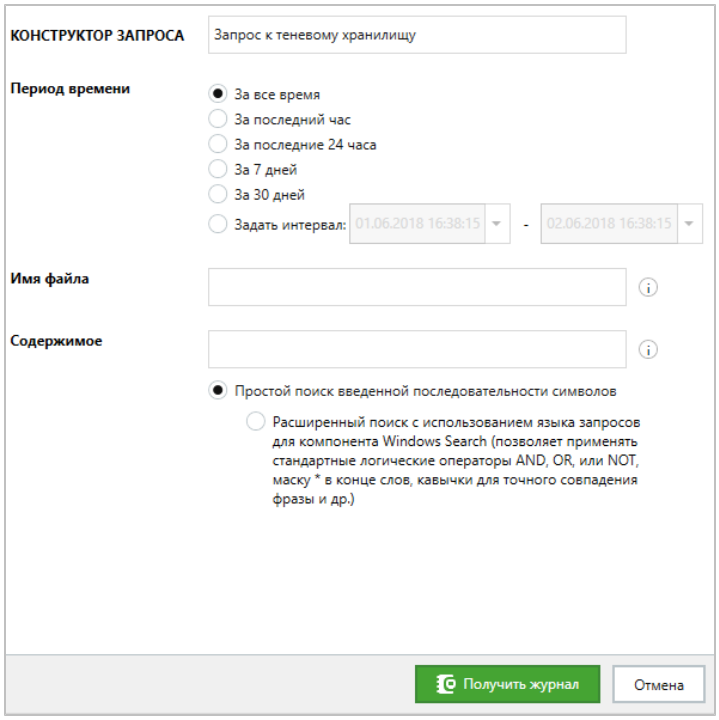
Настройка параметров запроса для поиска в хранилище теневого копирования

Программа управления в локальном режиме 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 настройки параметров запроса записей:

1. В панели управления запросами выберите команду "Новый | Запрос к теневому хранилищу".

   На экране появится панель настройки параметров запроса.



2. В поле "Конструктор запроса" введите имя запроса.
3. Настройте следующие параметры:

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.**82**). 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.**82**)
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

4. Нажмите кнопку "Получить журнал".

   Будет выполнен поиск нужных записей журнала и в области отображения сведений появится список найденных записей о событиях теневого копирования. Порядок работы с найденными записями и относящимися к ним файлами подробно описан в процедуре на стр.**86**.

Просмотр хранилища теневого копирования

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 программы управления в локальном режиме.

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 программы 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.

Создание временной копии файла

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.

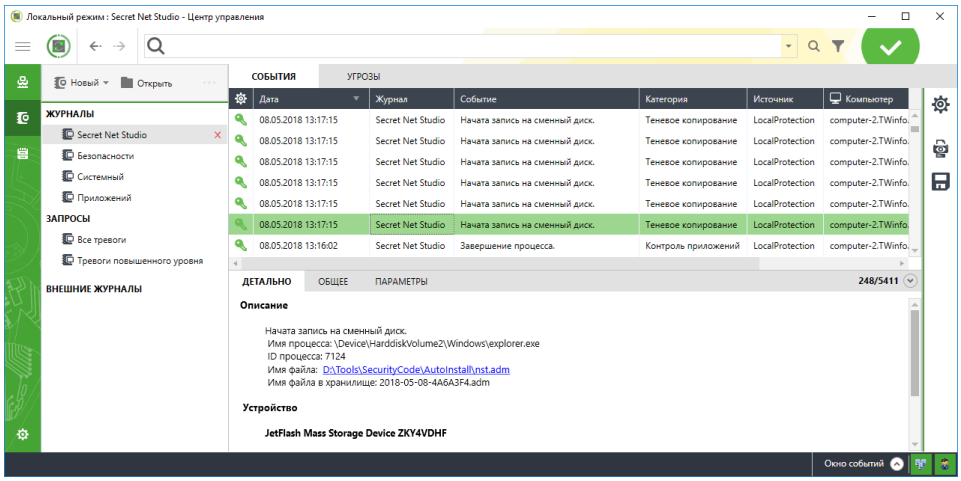
Программа управления в локальном режиме предоставляет возможность создать нужный файл с исходным именем и выполнить быстрый переход к этому файлу. Такой файл создается во временной папке хранилища на основе файла дубликата. Для создания используется запись журнала Secret Net Studio, содержащая сведения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

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

Для открытия окна с временной копией файла в хранилище:

1. Загрузите в программу записи локального журнала Secret Net Studio.
2. 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.



3. 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.

Очистка локального журнала

Очистку (удаление записей) локального журнала можно выполнить при экспорте в evtx-файл (см. стр.**83**) или с помощью команды "Очистить журнал" в контекстном меню журнала (такая команда может применяться только для штатных журналов ОС Windows).

Глава 7
Дополнительные возможности локального администрирования

Редактирование учетной информации компьютера

В учетной информации компьютера могут быть указаны следующие сведения:

- название подразделения, в котором используется компьютер;
- наименование автоматизированной системы предприятия;
- место расположения компьютера;
- номер системного блока.

Ввод учетной информации можно выполнить при установке клиентского ПО системы Secret Net Studio или позже. Возможности редактирования учетной информации предоставляются в программе управления (см. документ [**4**]), а также в диалоговом окне "Управление Secret Net Studio".

Для редактирования учетной информации в диалоговом окне "Управление Secret Net Studio":

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

   На экране появится диалоговое окно "Управление Secret Net Studio".
2. Перейдите к диалогу "Учетная информация".
3. Введите сведения о компьютере в соответствующих полях.
4. Нажмите кнопку "Применить" или "ОК".

Локальное оповещение о событиях тревоги

Событиями тревоги считаются события, которые регистрируются в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки". При возникновении на компьютере таких событий система защиты может локально оповещать об этом текущего пользователя компьютера.

Режим локального оповещения о событиях тревоги можно включать и отключать для всех пользователей компьютера (компьютеров) или предоставить пользователям возможность управлять режимом самостоятельно.

Ниже приводится описание процедуры централизованной настройки на рабочем месте администратора в программе управления (см. стр. **11**). Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме.

Для управления режимом локального оповещения о событиях тревоги:

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.

   Примечание.
   Сведения об использовании программы управления см. в документе [**4**].
2. В разделе "Политики" перейдите к группе параметров "Оповещение о тревогах".

3. Для параметра "Локальное оповещение о тревогах" укажите режим действия или выберите значение "Определяется пользователем".

Примечание.
Переключение режима локального оповещения пользователем осуществляется с помощью команды "Уведомления о тревогах" в контекстном меню пиктограммы Secret Net Studio, находящейся в панели задач Windows.

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

Локальная регистрация лицензий

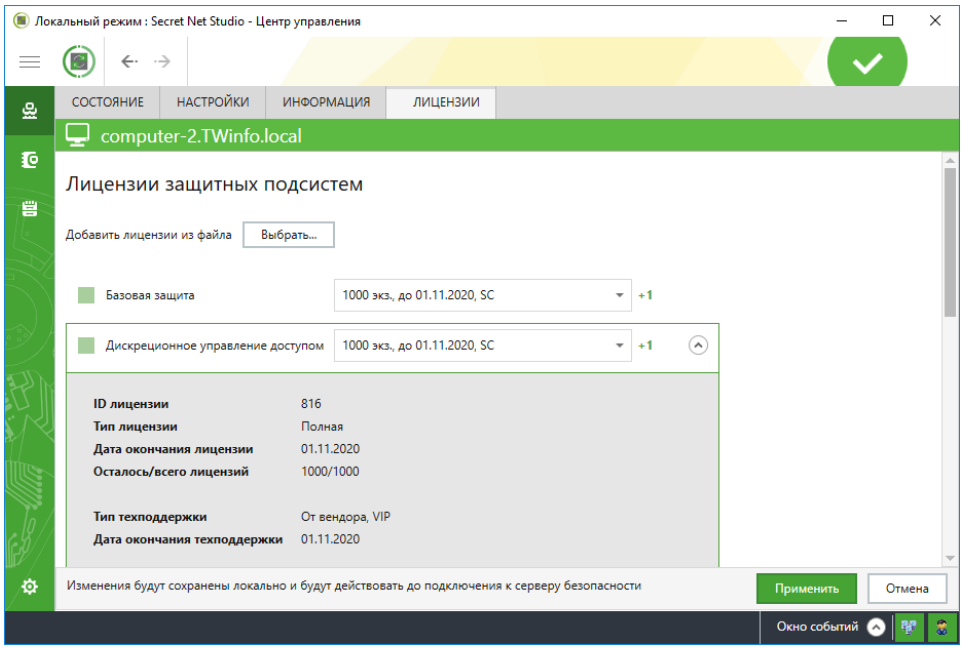
В системе Secret Net Studio действуют лицензионные ограничения на использование ряда подсистем, реализующих применение механизмов защиты. Регистрация лицензий осуществляется с помощью специальных файлов.

Для клиентов Secret Net Studio в сетевом режиме работы лицензии регистрируются на сервере безопасности. При подключении клиента к серверу происходит проверка лицензионных условий, и соответствующая клиентская лицензия загружается с сервера безопасности в локальное хранилище клиента. Регистрация лицензий на сервере безопасности выполняется в программе управления в централизованном режиме работы (см. документ [**4**]).

Также в системе предусмотрена локальная регистрация лицензий на защищаемых компьютерах. Локальная регистрация может потребоваться для клиента в автономном режиме работы, а также и в сетевом режиме, если подключение к серверу безопасности невозможно длительное время.

Для локальной регистрации лицензий:

1. Загрузите программу управления в локальном режиме (см. стр.**11**).
2. Откройте панель "Компьютер" и перейдите на вкладку "Лицензии".



На вкладке представлен список лицензируемых подсистем и сведения о текущем состоянии лицензий. Активированные подсистемы (с действующими лицензиями) имеют отметки слева от названий. Чтобы отобразить подробные сведения о лицензии на подсистему, наведите на строку с названием подсистемы и нажмите кнопку, которая появляется в выделенной строке справа.

3. При наличии файла с лицензиями, которые нужно зарегистрировать, нажмите кнопку "Выбрать", которая расположена над списком лицензируемых подсистем. В появившемся диалоге выбора файла выберите нужный файл с лицензиями.

После обработки данных список лицензий будет обновлен.

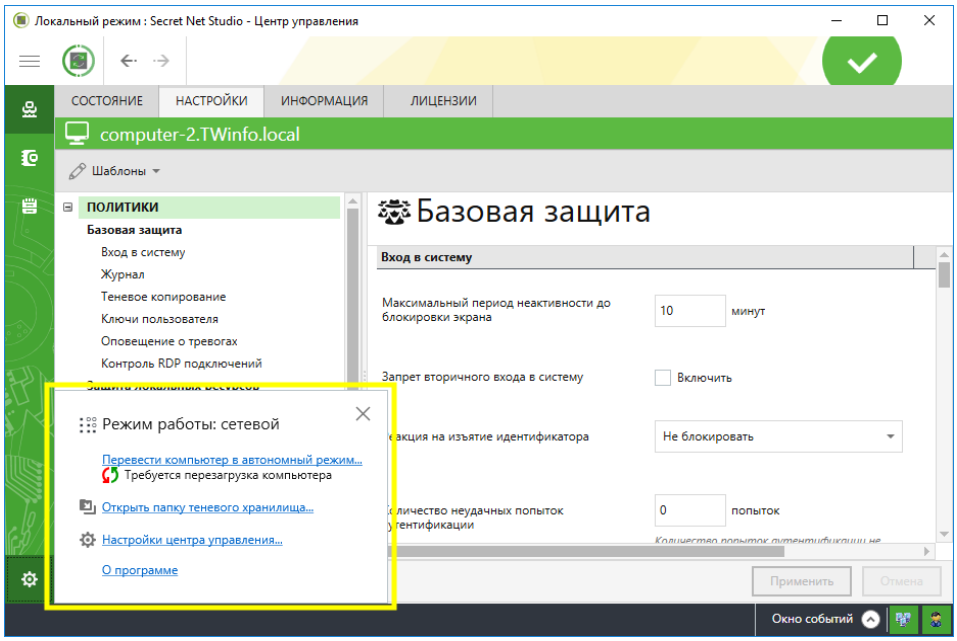
4. Для управления активацией подсистем (включение и отключение действия лицензий) используйте элементы управления, расположенные слева от названий подсистем. При отключении действия лицензии поле со сведениями о лицензии для подсистемы становится пустым и ниже выводится сообщение об удалении лицензии.
5. Для сохранения текущей конфигурации лицензий нажмите кнопку "Применить" в нижней части вкладки.

Изменение режима работы клиента

Клиент системы Secret Net Studio может функционировать в автономном и сетевом режимах (см. документ [**1**]). Текущий режим работы клиента отображается в программе управления. Переключение между режимами можно выполнить в программе управления и с использованием командной строки.

Для просмотра информации о текущем режиме работы клиента:

1. Запустите программу управления в локальном режиме (см. стр.**11**).
2. В нижней части панели навигации нажмите кнопку "Настройки". На экране появится панель вызова средств настройки:



В верхней части панели вызова средств настройки отобразится режим работы клиента:

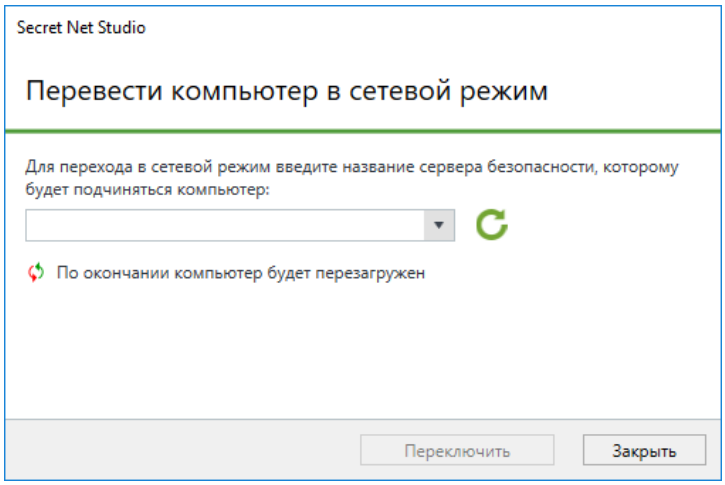
- "Режим работы: автономный" — при функционировании клиента в автономном режиме;
- "Режим работы: сетевой" — при функционировании клиента в сетевом режиме;
- "Режим работы: идет определение режима" — при выполнении процесса определения режима;
- "Режим работы: не определен" — при возникновении ошибок в процессе определения режима.

> **Пояснение.**
> Если режим работы клиента не определен, перезагрузите компьютер.

Для переключения клиента из автономного режима в сетевой:

1. Запустите программу управления в локальном режиме (см. стр.**11**).
2. В нижней части панели навигации нажмите кнопку "Настройки" и выберите команду "Перевести компьютер в сетевой режим...".

На экране появится окно с запросом учетных данных сервера безопасности.



3. Укажите наименование сервера безопасности, которому должен подчиняться клиент, одним из следующих способов:
   - нажмите кнопку для поиска доступных серверов безопасности и выберите необходимый сервер из списка найденных;
   - введите наименование сервера безопасности самостоятельно.
4. Нажмите кнопку "Переключить".

Пояснение.
Для отмены перехода в сетевой режим нажмите кнопку "Закрыть".

Начнется процесс проверки учетных данных сервера безопасности. Возможны следующие ошибки:

- наименование сервера безопасности введено неверно. В этом случае система выдаст сообщение об ошибке. Нажмите "Закрыть" и повторите процедуру;

  Пояснение.
  Если наименование сервера безопасности введено неверно, в журнале будет зарегистрировано событие "Ошибка. Входной параметр имеет нулевое значение. Сервер не найден".
- недостаточно прав для подчинения клиента серверу безопасности. В этом случае система выдаст сообщение об ошибке. Нажмите "ОК" и повторите процедуру с правами администратора домена безопасности.

При успешном завершении проверки учетных данных сервера безопасности начнется процесс настройки клиента для работы в сетевом режиме.

Пояснение.
При переводе клиента из автономного режима работы в сетевой система Secret Net Studio выполняет следующие действия:
- создает учетную запись клиента в структуре централизованного управления;
- создает запись о сервере безопасности в реестре клиента;
- вводит ключ активации лицензии клиента;
- подключает клиента к домену безопасности;
- переводит механизмы защиты клиента в сетевой режим работы.

При успешном завершении процесса настройки появится окно с сообщением о переводе клиента в сетевой режим и необходимости перезагрузить компьютер.

5. Нажмите кнопку "Перезагрузить".

Клиент будет переведен в сетевой режим. Выполнится проверка лицензии клиента. При возникновении ошибки лицензирования система выдаст соответствующее сообщение. В этом случае скорректируйте лицензии в программе управления, запущенной в централизованном режиме.

Пояснение.
Для переключения клиента из автономного режима в сетевой в командной строке перейдите в каталог установки клиента и выполните команду:

```
medusa.exe /switchmode=network /omserverName=<SERVERNAME>
/omserverPort=<PORT>
```

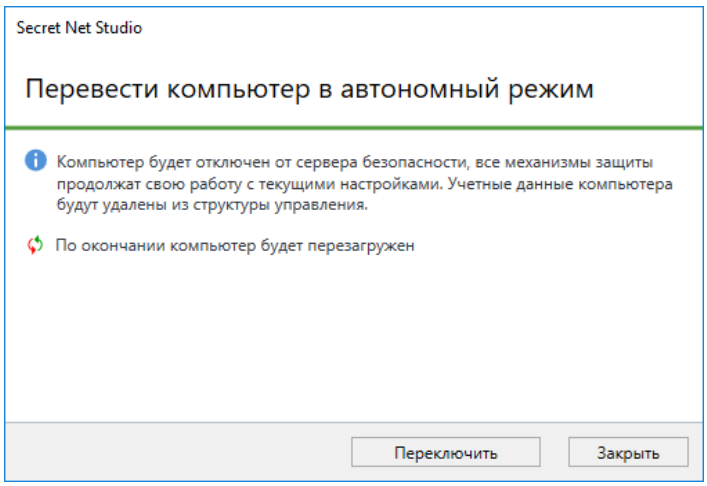
где:

- <SERVERNAME> — имя сервера безопасности, которому должен подчиняться клиент;
- <PORT> — порт сервера безопасности. Если параметр не задан, будет использоваться порт 443.

Для переключения клиента из сетевого режима в автономный:

1. Запустите программу управления в локальном режиме (см. стр.**11**).
2. В нижней части панели навигации нажмите кнопку "Настройки" и выберите команду "Перевести компьютер в автономный режим...".

   На экране появится предупреждение:



   Пояснение.
   При переводе клиента из сетевого режима работы в автономный система Secret Net Studio выполняет следующие действия:
   - удаляет учетные данные о клиенте из структуры централизованного управления;
   - переводит механизмы защиты клиента в автономный режим работы с сохранением текущих настроек и лицензии;
   - удаляет учетные данные сервера безопасности из локальной БД клиента.

3. Нажмите кнопку "Переключить".

   Пояснение.
   Для отмены перехода в автономный режим нажмите кнопку "Закрыть".

   Начнется процесс настройки клиента для работы в автономном режиме.

   При успешном завершении процесса настройки появится окно с сообщением о переводе клиента в автономный режим и необходимости перезагрузить компьютер.

   Пояснение.
   При переходе в автономный режим учетные данные о клиенте могут не удалиться из структуры управления автоматически. В этом случае система выдаст соответствующее предупреждение. После перевода клиента в автономный режим удалите учетные данные самостоятельно.

4. Нажмите кнопку "Перезагрузить".

   Клиент будет переведен в автономный режим.

Пояснение.
Для переключения клиента из сетевого режима в автономный в командной строке перейдите в каталог установки клиента и выполните команду:

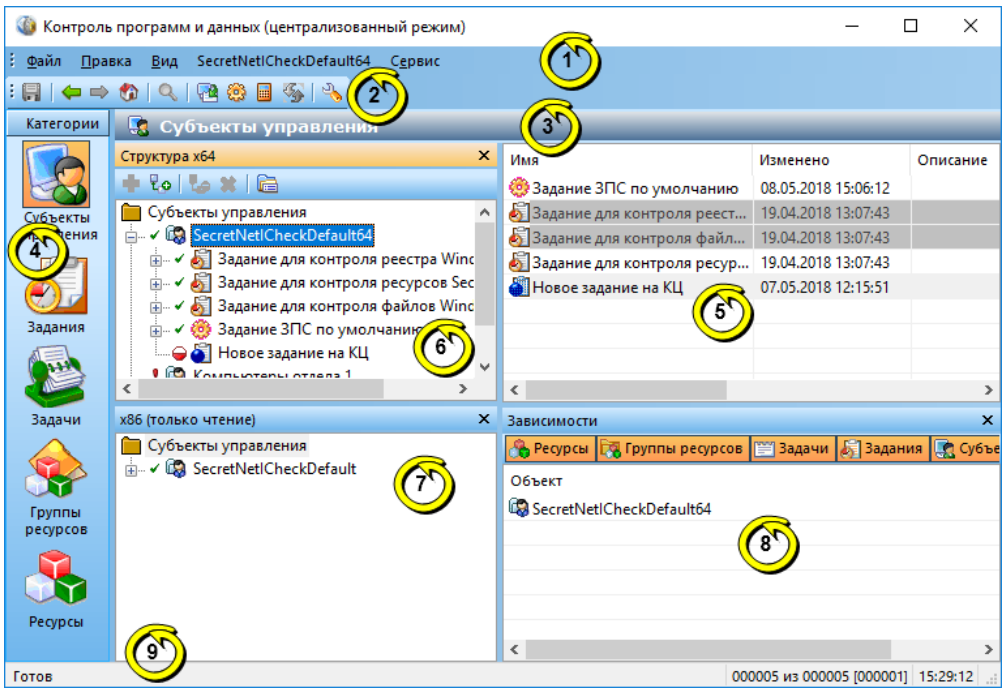
```
medusa.exe /switchmode=standalone
```

Приложение

Общие сведения о программе "Контроль программ и данных"

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.**95**)
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.

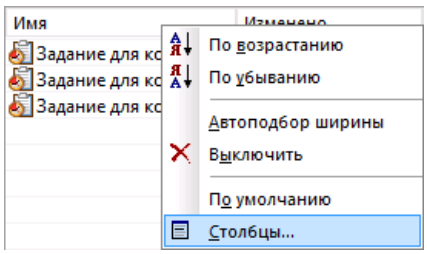
Команда	Кнопка	Описание
Вид | Назад		Выполняет переход к предыдущему выбранному элементу структуры
Вид | Вперед		Выполняет переход к следующему выбранному элементу структуры
Вид | Домой		Выполняет переход к корневому элементу структуры

Настройка отображения колонок в таблицах

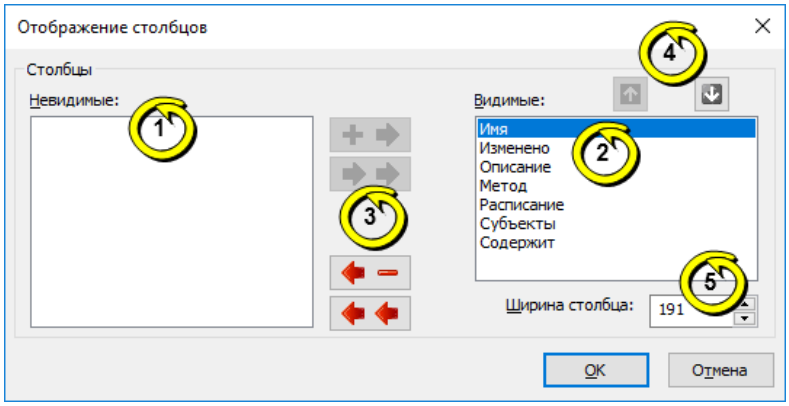
В области списка объектов и в окне зависимостей используется табличная форма представления списков объектов. Состав колонок таблицы зависит от того, объекты какой категории отображаются. Для оптимального отображения информации можно изменять ширину колонок, добавлять или удалять колонки либо перемещать 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.**94**).

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.

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 установки 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.

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, то 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 отличаться 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.

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.

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 [**2**]). 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.

Документация

1. Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
2. Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
3. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.001 91 3
4. Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
5. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
6. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
7. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
8. Средство защиты информации Secret Net Studio. Руководство администратора. Сервер обновлений. Установка и настройка	
9. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92