Средство защиты информации Secret Net 7
Сведения о вспомогательных утилитах и файлах настройки

Данный документ содержит общие описания вспомогательных утилит и файлов настройки (далее — вспомогательные средства) для выполнения специфических действий в СЗИ Secret Net 7. В зависимости от назначения и методов использования вспомогательные средства могут быть включены в комплект поставки или предоставляются отдельно.

Оглавление

1. Средства для работы с хранилищем объектов ЦУ

1.1. Файлы для создания резервной копии хранилища объектов ЦУ

Назначение, возможности

Файлы сценариев BackupServerData2008_2012.vbs и BackupServerData2003.vbs предназначены для резервного копирования информации о лесе доменов безопасности и о конкретном домене безопасности при размещении хранилища объектов централизованного управления вне Active Directory.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\BackupServerData\.

Условия использования

Сервер безопасности должен быть установлен с размещением хранилища объектов централизованного управления вне Active Directory.

Описание применения

При размещении хранилища объектов централизованного управления вне Active Directory сервер безопасности использует базу данных альтернативной службы каталогов. В зависимости от операционной системы компьютера сервера безопасности вместо доменных служб AD обработку данных осуществляют службы облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS) или компонент режима приложений Active Directory (Active Directory Application Mode, ADAM).

При резервном копировании сохраняются файлы данных AD LDS/ADAM и конфигурационный файл сервера безопасности. Сведения о восстановлении из резервной копии приведены в документе "Система защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

Резервное копирование выполняется с использованием программы-активатора сценариев CScript.exe из состава ОС. Перед созданием резервной копии необходимо подготовить отдельный каталог, в который будут записаны файлы.

В зависимости от версии операционной системы на компьютере сервера безопасности используется соответствующий файл сценария: BackupServerData2008_2012.vbs для Windows Server 2012/2008 или BackupServerData2003.vbs для Windows Server 2003. Формат запуска:

CScript.exe <*имя_vbs-файла_сценария*> <*каталог_для_резервной_копии*>

Примеры

- CScript.exe BackupServerData2008_2012.vbs c:\BackupLDS — выполняется резервное копирование в каталог c:\BackupLDS на компьютере под управлением ОС Windows Server 2012/2008.
- CScript.exe BackupServerData2003.vbs c:\BackupLDS — резервное копирование в каталог c:\BackupLDS на компьютере под управлением ОС Windows Server 2003.

1.2. Утилита для локального конфигурирования клиента Secret Net

Назначение, возможности

Утилита SnLDAPConfig.exe предназначена для локального конфигурирования клиента Secret Net в сетевом режиме функционирования для работы в структуре оперативного управления. Данное средство можно использовать, например, для подчинения компьютера серверу безопасности с хранилищем объектов централизованного управления вне Active Directory, если клиент был установлен без подчинения СБ или ранее был подчинен серверу с хранилищем объектов ЦУ в AD. Утилита может функционировать в графическом режиме или в режиме командной строки.

Утилита предоставляет следующие возможности:

- отображение сведений о текущей конфигурации и списка доступных серверов безопасности (только при работе в графическом режиме);
- регистрация компьютера в структуре ОУ;
- подчинение серверу безопасности;
- регистрация серийного номера клиента.

Размещение

Каталог установки клиента Secret Net.

Условия использования

Для работы с утилитой требуются права локального администратора. Дополнительно для выполнения действий могут потребоваться права на конфигурирование каталога LDAP (предоставляется возможность указать учетные данные соответствующего пользователя) и остановка работы службы "Secret Net Agent". Например, при подчинении компьютера другому серверу безопасности. После выполнения конфигурационных действий следует заново запустить службу "Secret Net Agent", если она была остановлена.

Описание применения

При запуске исполняемого файла без указания дополнительных параметров утилита функционирует в графическом режиме (описание использования в графическом режиме см. в документе "Система защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление"). Для режима командной строки используется следующий формат запуска:

SnLDAPConfig.exe /server:<*DNS-имя_сервера*> [/nosubordinate] [/noadd] [/license:local | /license:server | /license:<*серийный_номер*>] [/user:<*имя_пользователя*> /password:<*пароль*>]

Описание параметров команды:

- /server:<*DNS-имя_сервера*> — выполняет подключение к указанному серверу безопасности. Обязательный параметр для режима командной строки. Если другие параметры не указаны, выполняется подчинение компьютера указанному серверу, получение от этого сервера серийного номера и сохранение его в локальном хранилище.
- /nosubordinate — отменяет подчинение серверу и считывание серийного номера.
- /noadd — отменяет все другие параметры, происходит только запись в системный реестр данных для подключения к указанному серверу.
- /license: — выполняет регистрацию серийного номера. Предусмотрены следующие варианты:
  - /license:local — регистрация в централизованном хранилище СНК, имеющегося на этом компьютере;
  - /license:server — получение СНК с сервера;

  - /license:<*серийный_номер*> — регистрация нового СНК.
- /user: и /password: — учетные данные пользователя с правами на конфигурирование каталога LDAP.

Примеры

- SnLDAPConfig.exe /server:SnLDSServer1.SnDomain.ru — выполняется подчинение серверу безопасности SnLDSServer1.SnDomain.ru, получение серийного номера клиента с сервера и сохранение СНК в локальном хранилище.
- SnLDAPConfig.exe /server:SnADServer.SnDomain.ru /license:local — выполняется подчинение серверу безопасности SnADServer.SnDomain.ru и регистрация в централизованном хранилище серийного номера клиента, сохраненного локально.

1.3. Утилита управления централизованными параметрами безопасности Secret Net

Назначение, возможности

Утилита SnDSTool.exe предназначена для выполнения действий с хранилищем объектов централизованного управления и предоставляет следующие возможности:

- включение разрешения разового входа в систему для всех пользователей, которые не имеют сохраненного пароля в БД Secret Net (автоматическая установка параметра "Доверять парольной аутентификации Windows при следующем входе в систему" для режима усиленной аутентификации по паролю);
- очистка хранилища от сведений о неиспользуемых идентификаторах, которые остаются, например, после удаления доменного пользователя с присвоенными идентификаторами на компьютере без установленного клиентского ПО системы Secret Net;
- вывод сведений о зарегистрированных лицензиях на использование компонентов системы Secret Net;
- вывод сведений о доменах безопасности при размещении хранилища объектов ЦУ вне Active Directory.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\SnDSTool\.

Условия использования

В зависимости от выполняемой операции сервер безопасности должен быть установлен с соответствующим размещением хранилища объектов централизованного управления (в Active Directory или в БД альтернативной службы каталогов). Для работы с доменом безопасности на компьютере должен быть установлен клиент системы Secret Net с подчинением серверу безопасности.

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске без параметров или с параметром –? выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- SnDSTool.exe –settrust — для пользователей текущего домена Active Directory выполняется автоматическая установка параметра "Доверять парольной аутентификации Windows при следующем входе в систему" (исключая тех пользователей, пароль которых сохранен в БД Secret Net).
- SnDSTool.exe –lds –settrust — для пользователей домена безопасности, параметры соединения с которым хранятся в системном реестре, выполняется автоматическая установка параметра "Доверять парольной аутентификации Windows при следующем входе в систему" (исключая тех пользователей, пароль которых сохранен в БД Secret Net). Команда применяется, если сервер безопасности установлен с размещением хранилища объектов ЦУ вне AD.
- SnDSTool.exe –duei — выполняется очистка от сведений о неиспользуемых идентификаторах в текущем домене Active Directory (применяется, если сервер безопасности установлен с размещением хранилища объектов централизованного управления в AD).
- SnDSTool.exe –lds –duei — выполняется очистка от сведений о неиспользуемых идентификаторах в домене безопасности, параметры соединения с которым хранятся в системном реестре (применяется, если сервер безопасности установлен с размещением хранилища объектов ЦУ вне AD). Необходимые параметры соединения присутствуют в системном реестре при условии, что на компьютере установлен клиент системы Secret Net с подчинением серверу безопасности.
- SnDSTool.exe –lds snldssrv –pds — выводится список имен всех доменов безопасности в лесу, где размещается сервер безопасности с именем snldssrv (применяется, если сервер безопасности установлен с размещением хранилища объектов ЦУ вне AD).

- SnDSTool.exe –lds snldssrv DC={d0b4ad49-e896-4ab0-a557-b66200a8ffbe},DC=SecretNet-GC –duei — выполняется очистка от сведений о неиспользуемых идентификаторах в указанном домене безопасности (применяется, если сервер безопасности snldssrv установлен с размещением хранилища объектов ЦУ вне AD). Домен безопасности должен быть указан в формате имени distinguished name (DN). DN-имена доменов выводятся, например, в результатах выполнения предыдущей команды.
- SnDSTool.exe –pli — выводятся сведения о всех лицензиях системы Secret Net, зарегистрированных в хранилище.

2. Средства для расширения возможностей администраторов безопасности

2.1. Файлы для регистрации конфигурационных данных в каталоге Active Directory

Назначение, возможности

Набор файлов, состоящий из командного файла sn7-modify-AD.cmd и дополнительных файлов, предназначен для регистрации конфигурационных данных системы Secret Net в разделе конфигурации каталога Active Directory. После регистрации конфигурационные данные обеспечивают возможность управления параметрами Secret Net для доменных пользователей с использованием стандартных оснасток ОС Windows.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\ModifyAD\.

Условия использования

Регистрация конфигурационных данных с использованием набора файлов выполняется от имени пользователя с правами на изменение конфигурации каталога AD. По умолчанию такие права предоставлены пользователям группы "Администраторы предприятия" (Enterprise Admins).

Примечание: Регистрацию конфигурационных данных с помощью файла sn7-modify-AD.cmd не требуется выполнять в следующих случаях:

- если сервер безопасности устанавливается с размещением хранилища объектов ЦУ в БД Active Directory. В этом случае должна выполняться модификация схемы AD, во время которой также регистрируются конфигурационные данные;
- если установку сервера безопасности с размещением хранилища объектов ЦУ вне Active Directory будет выполнять пользователь с правами на изменение конфигурации каталога AD. По умолчанию такие права предоставлены пользователям группы "Администраторы предприятия" (Enterprise Admins);
- если настройка параметров пользователей будет осуществляться в программе управления пользователями из состава ПО клиента системы Secret Net (без использования стандартной оснастки "Active Directory — пользователи и компьютеры").

Описание применения

Для регистрации данных запустите на исполнение командный файл sn7-modify-AD.cmd.

2.2. Утилита для делегирования административных полномочий пользователям

Назначение, возможности

Утилита SnDelegate.exe предназначена для предоставления администраторам безопасности необходимых прав для управления объектами в организационных подразделениях. Утилита задает фиксированный набор прав для учетной записи к объектам указанного организационного подразделения.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\SnDelegate\.

Условия использования

Утилиту SnDelegate.exe может использовать пользователь, который обладает полномочиями для делегирования административных полномочий (например, администратор домена).

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя (по умолчанию). При необходимости можно указать учетные данные другого пользователя. При запуске без параметров или с параметром –? выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- SnDelegate -o "Secret Net Admin Delegated" -u Ivanov — пользователю Ivanov предоставляются права на управление объектами организационного подразделения "Secret Net Admin Delegated".

3. Средства для работы с СУБД

3.1. Файлы для очистки БД сервера безопасности в СУБД Oracle

Назначение, возможности

Набор файлов, состоящий из командных файлов clear.cmd, rebuild.cmd и дополнительных файлов в каталоге \Tools\Infosec\ClearOracle\, предназначен для очистки базы данных сервера безопасности, размещенной на сервере СУБД Oracle. Процедура очистки БД может потребоваться для восстановления работы сервера СУБД Oracle в случае переполнения БД сервера безопасности.

Рекомендации

Регулярно выполняйте архивирование журналов в базе данных сервера и другие необходимые действия для поддержания приемлемого объема базы данных. Очистку БД с использованием указанных файлов следует выполнять только в случае, если произошло переполнение БД и сервер безопасности не может продолжать функционировать. Очистка приведет к потере всей хранящейся в БД информации, включая содержимое журналов, поступивших на централизованное хранение.

На сервере СУБД рекомендуется периодически запускать команду перестроения индексов с использованием файла rebuild.cmd. При длительной эксплуатации и частом архивировании БД производительность сервера снижается из-за сильной фрагментации данных. Процедура перестроения индексов не требует остановки функционирования сервера, однако для оптимального быстродействия рекомендуется запускать команду в моменты наименьшей нагрузки.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\ClearOracle\.

Условия использования

Для выполнения процедуры очистки БД требуются права локального администратора на компьютере сервера безопасности и учетные данные администратора БД в СУБД Oracle.

Описание применения

Для очистки базы данных сервера безопасности выполните следующие действия:

1. На сервере безопасности остановите работу служб IIS (служба веб-публикации) и Secret Net Security Server (служба сервера, прежнее название — Operation Management System Server).

2. На сервере Oracle создайте каталог на локальном диске и скопируйте в него с компакт-диска комплекта поставки содержимое каталога \Tools\Infosec\ClearOracle\.

3. Откройте для редактирования скопированные файлы с расширением *.cmd и укажите в них пароль администратора БД, заданный при установке сервера СУБД. Пароль должен быть указан вместо подстроки oracle.

4. Запустите на исполнение отредактированный файл clear.cmd. После успешного завершения обработки этого файла запустите файл rebuild.cmd.

5. Перезагрузите сервер безопасности.

3.2. Файлы для очистки БД сервера безопасности в СУБД MS SQL

Назначение, возможности

Набор файлов, состоящий из командных файлов clear.cmd, rebuild.cmd и дополнительных файлов в каталоге \Tools\Infosec\ClearMSSQL\, предназначен для очистки базы данных сервера безопасности, размещенной на сервере СУБД MS SQL. Процедура очистки БД может потребоваться для восстановления работы сервера СУБД MS SQL в случае переполнения БД сервера безопасности.

Рекомендации

Регулярно выполняйте архивирование журналов в базе данных сервера и другие необходимые действия для поддержания приемлемого объема базы данных. Очистку БД с использованием указанных файлов следует выполнять только в случае, если произошло переполнение БД и сервер безопасности не может продолжать функционировать. Очистка приведет к потере всей хранящейся в БД информации, включая содержимое журналов, поступивших на централизованное хранение.

На сервере СУБД рекомендуется периодически запускать команду перестроения индексов с использованием файла rebuild.cmd. При длительной эксплуатации и частом архивировании БД производительность сервера снижается из-за сильной фрагментации данных. Процедура перестроения индексов не требует остановки функционирования сервера, однако для оптимального быстродействия рекомендуется запускать команду в моменты наименьшей нагрузки.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\ClearMSSQL\.

Условия использования

Для выполнения процедуры очистки БД требуются права локального администратора на компьютере сервера безопасности и учетные данные администратора БД в СУБД MS SQL.

Описание применения

Для очистки базы данных сервера безопасности выполните следующие действия:

1. На сервере безопасности остановите работу служб IIS (служба веб-публикации) и Secret Net Security Server (служба сервера, прежнее название — Operation Management System Server).

2. На сервере MS SQL создайте каталог на локальном диске и скопируйте в него с компакт-диска комплекта поставки содержимое каталога \Tools\Infosec\ClearMSSQL\.

3. Откройте для редактирования скопированные файлы с расширением *.cmd и укажите в них пароль администратора БД, заданный при установке сервера СУБД. Пароль должен быть указан вместо подстроки manager.

4. Запустите на исполнение отредактированный файл clear.cmd. После успешного завершения обработки этого файла запустите файл rebuild.cmd.

5. Перезагрузите сервер безопасности.

4. Средства для клиентов Secret Net предыдущих версий

4.1. Параметры протокола TCP/IP по умолчанию

Назначение, возможности

Файл tcpip.reg предназначен для восстановления значений по умолчанию в стандартных параметрах системного реестра, которые регулируют использование протокола TCP/IP.

> **Примечание:** Изменение данных параметров выполнялось при установке клиентов системы Secret Net версий 5.X и 6.X. Программа установки клиента текущей версии не изменяет значения указанных параметров.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\DefNetReg\.

Условия использования

Для внесения изменений в системный реестр требуются права локального администратора.

Описание применения

Чтобы вернуть значения по умолчанию (если параметры были изменены при установке клиента Secret Net версии 5.X или 6.X), запустите редактор реестра и импортируйте содержимое файла tcpip.reg.

5. Средства для работы с журналом Secret Net

5.1. Утилита для экспорта в файл содержимого журнала Secret Net

Назначение, возможности

Утилита GetEventLog.exe предназначена для экспорта в файл содержимого журнала Secret Net и предоставляет следующие возможности:

- экспорт записей в файл без очистки журнала;
- экспорт записей в файл с последующей очисткой журнала.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\GetEventLog\.

Условия использования

Создать файл с записями журнала Secret Net может пользователь с привилегией на просмотр журнала. При этом у пользователя должны быть права на запись файла в указанном размещении. Очистить журнал после экспорта может пользователь с привилегией на управление журналом.

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске без параметров или с параметром –? выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- GetEventLog.exe –a –n c:\EvtLog\SnEventLog.evt — выполняется экспорт записей из локального журнала в файл SnEventLog.evt без очистки содержимого журнала.

- GetEventLog.exe –c –n c:\EvtLog\SnEventLog.evt — выполняется экспорт записей из локального журнала в файл SnEventLog.evt с последующей очисткой содержимого журнала.

6. Средства для подсистем контроля целостности и замкнутой программной среды

6.1. Утилита для работы с локальной БД КЦ-ЗПС

Назначение, возможности

Утилита SnIcheckCmdTool.exe предназначена для выполнения действий с локальной БД КЦ-ЗПС, в которой хранится модель данных, и предоставляет следующие возможности:

- запуск полной синхронизации изменений, сделанных в центральной БД КЦ-ЗПС;
- подготовка ресурсов для ЗПС;
- вывод сведений об объектах группы по умолчанию при размещении хранилища объектов централизованного управления вне Active Directory;
- перерасчет эталонов ресурсов;
- обновление хранилищ эталонов, содержащих зафиксированные эталонные значения ресурсов Secret Net для метода контроля "Содержимое" и алгоритма CRC7 (используются при контроле целостности ресурсов Secret Net и могут быть заменены только при установке авторизованных обновлений ПО системы защиты).

Размещение

Каталог установки клиента Secret Net.

Условия использования

Для работы с утилитой требуются права локального администратора.

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске без параметров выводятся основные сведения об использовании утилиты. Формат запуска:

SnIcheckCmdTool.exe /<*параметр*>

Предусмотрены следующие параметры запуска:

- /fullsync — запуск полной синхронизации изменений в ЦБД КЦ-ЗПС.
- /fullsynccentral — запуск полной синхронизации изменений в ЦБД КЦ-ЗПС с использованием функции рассылки оповещений об изменениях для данного компьютера (компьютер должен быть представлен в централизованной модели данных в качестве отдельного субъекта).
- /reloaduel — запуск процедуры подготовки ресурсов для ЗПС. Процедура выполняется для всех пользователей, имеющих открытые сеансы работы на данном компьютере в текущий момент.
- /defgroup — вывод списка идентификаторов безопасности (SID) компьютеров, входящих в группу по умолчанию SecretNetICheckDefault или SecretNetICheckDefault64 (в зависимости от разрядности версии ОС на компьютере). Список составляется при размещении хранилища объектов централизованного управления вне Active Directory.
- /recalc — перерасчет эталонных значений указанного ресурса для метода контроля "Содержимое" и алгоритма CRC7 и сохранение их в ЛБД КЦ-ЗПС.
- /etalon — запись новых эталонных значений указанного ресурса в локальную базу эталонов дистрибутива СЗИ Secret Net. База содержит зафиксированные эталоны всех ресурсов Secret Net для метода контроля "Содержимое" и алгоритма CRC7.

При запуске с параметрами /recalc, /etalon необходимо указать дополнительные атрибуты. Сведения об использовании утилиты с указанными параметрами (формат запуска с описанием применяемых атрибутов) выводятся при запуске утилиты с параметром без атрибутов. Предусмотрены следующие атрибуты:

- тип ресурса:
  - f — файл;
  - c — каталог;
  - k — ключ реестра;
  - v — параметр реестра;
  - a — все файлы в каталоге;
  - r — все параметры в ключе реестра;
- путь к ресурсу;

- назначение:
  - w — атрибут должен быть выставлен при расчете контрольных сумм для 32-разрядных исполняемых файлов, предназначенных для использования в 64-разрядных ОС (не используется для параметра /recalc).

Примеры

- SnIcheckCmdTool.exe /fullsync — выполняется полная синхронизация модели данных на компьютере.
- SnIcheckCmdTool.exe /defgroup — выводится список SID компьютеров, входящих в группу по умолчанию SecretNetICheckDefault или SecretNetICheckDefault64 (в зависимости от разрядности версии ОС на компьютере) при размещении хранилища объектов централизованного управления вне Active Directory.
- SnIcheckCmdTool.exe /recalc a c:\ — выполняется перерасчет эталонных значений всех файлов в корневом каталоге диска C: и их сохранение в ЛБД КЦ-ЗПС. Перерасчет выполняется для эталонов, рассчитанных по алгоритму CRC7.

7. Средства для подсистемы полномочного управления доступом

7.1. Утилита для изменения категорий конфиденциальности файловых ресурсов

Назначение, возможности

Утилита SetSecAttrib.exe предназначена для изменения категорий конфиденциальности каталогов и файлов и предоставляет следующие возможности:

- присвоение категории конфиденциальности файловому ресурсу;
- присвоение категории конфиденциальности вложенным ресурсам (если утилита применяется для каталога);
- изменение параметров наследования категорий конфиденциальности для вложенных ресурсов (если утилита применяется для каталога).

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\SetSecAttrib\.

Условия использования

Присвоить категорию конфиденциальности может пользователь с привилегией на управление категориями конфиденциальности. Категория указывается в виде порядкового номера от 0 (соответствует категории для общедоступной информации) до 15 (соответствует наивысшей категории).

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске с параметром –? выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- SetSecAttrib.exe -p "c:\temp" -s 1 -f 2 -r 0 — каталогу c:\temp присваивается категория конфиденциальности "конфиденциально" и для каталога включен параметр, определяющий присвоение этой категории всем вновь создаваемым вложенным файлам. При этом категории конфиденциальности имеющихся вложенных каталогов и файлов остаются без изменений.
- SetSecAttrib.exe -p "c:\temp" -s 2 -f 3 -r 2 — каталогу c:\temp присваивается категория конфиденциальности "строго конфиденциально" и для каталога включен параметр, определяющий присвоение этой категории всем вновь создаваемым вложенным каталогам. При этом данная категория присваивается всем вложенным каталогам и файлам.
- SetSecAttrib.exe -p "c:\temp\new.txt" -s 1 — файлу c:\temp\new.txt присваивается категория конфиденциальности "конфиденциально".

8. Средства для подсистемы контроля устройств

8.1. Утилита для управления аппаратной конфигурацией

Назначение, возможности

Утилита SnHwUtil.exe предназначена для работы со списком устройств компьютера и предоставляет следующие возможности:

- утверждение обнаруженных изменений в конфигурации устройств;
- проверка изменений в конфигурации устройств;
- загрузка актуального списка устройств;
- поиск и исправление недействительных записей в списке устройств;
- удаление явно заданных параметров контроля и прав доступа в списке устройств;
- удаление из списка устройств, которые отсутствуют на компьютере;
- экспорт списка устройств в файл.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\SnHwUtil\.

Условия использования

Для доступа к списку устройств требуются права локального администратора.

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске без параметров или с параметром –? выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- SnHwUtil.exe -c — утвердить обнаруженные изменения в аппаратной конфигурации.
- SnHwUtil.exe -v — найти и исправить недействительные записи в списке устройств.
- SnHwUtil.exe -r — удалить явно заданные параметры контроля и права доступа для всех устройств.

9. Прочие вспомогательные средства

9.1. Утилита для импорта параметров политики из файла шаблона

Назначение, возможности

Утилита SnetPol.exe предназначена для импорта параметров Secret Net из сохраненного файла-шаблона групповой политики в эффективную (результирующую) групповую политику на компьютере.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\SnetPol\.

Условия использования

Для доступа к параметрам политики требуются права локального администратора.

Описание применения

Утилита выполняет действия в режиме командной строки от имени текущего пользователя. При запуске без параметров или с параметром –h выводятся сведения об использовании утилиты (формат запуска с описанием применяемых параметров).

Примеры

- SnetPol -i "C:\TemplateFileName.inf" — выполняется импорт параметров Secret Net из файла-шаблона C:\TemplateFileName.inf в эффективную политику.

9.2. Параметры включения и отключения трассировки ПО

Назначение, возможности

Файлы trace_on.reg и trace_off.reg предназначены для изменения значений параметров системного реестра, определяющих включение и отключение трассировки. Трассировка — сервисная функция для сбора информации о работе системы Secret Net.

> **Примечание:** При включенной трассировке осуществляется запись служебных данных о функционировании программных модулей. Эти данные необходимы для диагностики возникновения сбойных или ошибочных ситуаций. Сведения о необходимых действиях предоставляются при обращении в отдел технической поддержки компании "Код Безопасности".

Рекомендации

Не включайте функцию трассировки без особой необходимости. В штатном режиме эксплуатации системы Secret Net данная функция должна быть отключена, чтобы не создавать лишнюю нагрузку для компьютера.

Размещение

Установочный компакт-диск системы Secret Net, каталог \Tools\Infosec\Trace\.

Условия использования

Для внесения изменений в системный реестр требуются права локального администратора.

Описание применения

Чтобы включить или отключить трассировку, запустите редактор реестра и импортируйте содержимое файла trace_on.reg или trace_off.reg соответственно.