Средство защиты информации Secret Net 7
Инструкция по делегированию административных полномочий

Данный документ содержит развернутое описание последовательности действий для делегирования административных полномочий на управление СЗИ Secret Net 7 в сетевом режиме функционирования.

1. Общие сведения

Делегирование подразумевает возложение некоторых функций по настройке и управлению работой механизмов защиты на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществляться только в рамках определенных организационных подразделений, созданных внутри домена.

Процедуру делегирования следует выполнять в случае, если хранилище объектов централизованного управления размещается в БД доменных служб Active Directory и при этом необходимо передать часть полномочий системных администраторов (администраторов домена) администраторам информационной безопасности.

Примечание: Для случая размещения хранилища объектов вне AD выполнять процедуру делегирования не требуется — достаточно включить администраторов безопасности в доменную группу Group Policy Creator Owners.

После делегирования администратор безопасности в рамках организационного подразделения (ОП) получает следующие права на управление СЗИ Secret Net (как и члены доменной группы администраторов):

- установка и удаление компонента "Secret Net 7" в сетевом режиме функционирования;
- включение и отключение совместной работы с ПАК "Соболь";
- управление параметрами Secret Net для пользователей (в том числе присвоение и настройка идентификаторов, формирование списков компьютеров для входа в ПАК "Соболь");
- управление параметрами групповой политики ОП в оснастке ОС Windows;
- управление параметрами КЦ и ЗПС.

Однако не все полномочия могут быть делегированы администраторам безопасности. Следующие операции могут выполняться только членами доменной группы администраторов:

- установка и удаление компонента "Secret Net 7 — Сервер безопасности";
- редактирование подчиненности серверов безопасности и их параметров;
- генерация ключей централизованного управления ПАК "Соболь";
- управление режимом интеграции с СЗИ TrustAccess.

Дополнительно пользователям могут быть назначены привилегии для работы с программой оперативного управления, входящей в состав ПО СЗИ Secret Net. Для выполнения действий в программе предусмотрены следующие типы привилегий пользователей:

- чтение и просмотр данных — дает возможность подключения к серверу безопасности;
- редактирование конфигурации сетевой структуры и свойств объектов;
- архивирование и восстановление централизованных журналов;
- выполнение команд оперативного управления;
- квитирование событий НСД;
- удаленная настройка параметров Secret Net на рабочих станциях.

2. Предварительные действия

Перед делегированием административных полномочий необходимо установить компонент "Secret Net 7 — Сервер безопасности" хотя бы на одном компьютере домена.

Рекомендации: Если в домене будет несколько серверов безопасности — рекомендуется установить компонент на все компьютеры, предназначенные для использования в этом качестве.

На компьютере, где будет выполняться настройка для делегирования, установите следующее ПО:

- средства централизованного управления ОС Windows (установлены по умолчанию на контроллере домена, на других компьютерах устанавливаются отдельно);
- компонент "Secret Net 7" в сетевом режиме функционирования;
- компонент "Secret Net 7 — Программа управления".

Примечание: Сведения об установке средств централизованного управления ОС Windows см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты". Сведения об установке компонентов СЗИ Secret Net см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

3. Порядок делегирования

Процедура делегирования выполняется пользователем с правами администратора домена.

1. Откройте оснастку "Active Directory — пользователи и компьютеры" и выберите в дереве объектов домен, в котором требуется делегировать административные полномочия. Создайте в домене одно или несколько организационных подразделений, в которых будут сгруппированы компьютеры и пользователи, управляемые администратором (администраторами) безопасности. Для создания ОП откройте меню "Действие" и активируйте команду "Создать | Подразделение". Также в этих целях можно использовать уже имеющиеся организационные подразделения.

2. В каждом организационном подразделении должны быть сформированы списки объектов для управления: компьютеры и учетные записи пользователей, включая администраторов безопасности. Недостающие объекты можно переместить из списка доменных учетных записей (компьютеров и пользователей) или создать непосредственно в объекте ОП — для этого выберите организационное подразделение, в меню "Действие" раскройте подменю "Создать" и активируйте соответствующую команду (например, "Пользователь").

Примечание: Списки объектов организационных подразделений можно формировать и редактировать в процессе эксплуатации системы. На данном этапе в ОП требуется как минимум создать учетные записи администраторов безопасности.

3. Включите администраторов безопасности в доменные группы "SecretNetAdmins" и "Group Policy Creator Owners". Для включения пользователя в группу выберите его и в меню "Действие" активируйте команду "Добавить в группу".

4. На локальном диске создайте папку C:\UtilSN и с установочного компакт-диска СЗИ Secret Net скопируйте в эту папку утилиту для настройки делегирования SnDelegate.exe. Утилита размещается в каталоге \Tools\Infosec\SnDelegate и представлена в отдельных вариантах для 32- и 64-разрядных версий ОС. Скопируйте файл, соответствующий разрядности операционной системы компьютера, на котором выполняется процедура делегирования.

Примечание: Папку можно создать на любом локальном диске компьютера. Имя и размещение папки не регламентируется. Далее в инструкции рассматривается папка C:\UtilSN.

5. С помощью утилиты предоставьте администраторам безопасности необходимые права на управление объектами. Для этого запустите консоль командной строки cmd.exe (если включен механизм управления учетными записями User Account Control — запуск необходимо выполнить от имени администратора) и для каждой учетной записи пользователя или группы введите команду C:\UtilSN\SnDelegate -o *<имя_ОП>* -u *<имя_администратора_безопасности_или_группы>*. После успешного завершения процесса предоставления прав можно удалить утилиту и папку C:\UtilSN.

Пример: Если пользователю Ivanov необходимо предоставить права на управление ОП "Secret Net Admin Delegated" — введите команду C:\UtilSN\SnDelegate -o "Secret Net Admin Delegated" -u Ivanov

Примечание: С помощью отдельных параметров запуска утилиты дополнительно можно указать имя альтернативного контроллера домена (если оно отличается от текущего контроллера домена по умолчанию) и учетные данные администратора домена (если текущий пользователь не обладает необходимыми правами). Чтобы вывести сведения о составе предусмотренных параметров утилиты, введите команду C:\UtilSN\SnDelegate -?

6. Назначьте администраторам безопасности привилегии для работы с программой оперативного управления. Для этого запустите программу в режиме конфигурирования и для каждого сервера безопасности на вкладке "Привилегии пользователей" сформируйте список учетных записей с привилегиями на управление данным сервером.

Примечание: Сведения о работе с программой оперативного управления см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления".

7. На всех рабочих местах администраторов безопасности проверьте состав локальных групп администраторов. В эти группы должны быть включены соответствующие учетные записи, которым делегированы административные полномочия. Учетные записи пользователей могут быть включены в локальные группы администраторов непосредственно или в составе других групп (например, как входящие в доменную группу "SecretNetAdmins"). Для просмотра и изменения состава локальной группы откройте оснастку "Управление компьютером", выберите группу администраторов и в меню "Действие" активируйте команду "Добавить в группу".