Средство защиты информации Secret Net 7
Инструкция по обновлению на Secret Net 7

Данный документ содержит описание последовательности действий для автоматизации и контроля процесса установки ПО Secret Net текущей версии с обновлением с предыдущих версий в следующих случаях:

- если необходимо выполнить обновление клиентов на компьютерах, подчиненных серверу безопасности с размещением хранилища объектов централизованного управления в Active Directory, в варианте последующего подчинения этих компьютеров серверу безопасности с размещением хранилища объектов ЦУ вне AD;
- если в системе развернута иерархия серверов безопасности версий до 6.5 включительно.

Во всех других случаях для выполнения и контроля автоматической установки клиентского ПО Secret Net на компьютерах можно использовать последовательность действий, которая приводится в документе "Инструкция по автоматической установке клиента Secret Net 7".

Перед обновлением необходимо выполнить начальную установку компонентов СЗИ Secret Net с помощью установочного компакт-диска СЗИ Secret Net текущей версии:

1. На всех компьютерах, где будет установлено программное обеспечение СЗИ Secret Net, должен быть указан русский язык в качестве языка программ, не поддерживающих Юникод. Проверьте выполнение данного требования на компьютерах. Для просмотра и изменения состояния параметра вызовите диалоговое окно "Язык и региональные стандарты" в Панели управления ОС Windows.

2. Если хранилище объектов централизованного управления будет размещаться в Active Directory, выполните модификацию схемы Active Directory.

3. На компьютерах, которые будут функционировать в качестве серверов безопасности, установите компонент "Secret Net 7 — Сервер безопасности".

> **Примечание:** При наличии в системе иерархии серверов безопасности версий до 6.5 включительно, чтобы последовательно обновить всю структуру без потери функциональности мониторинга и управления серверами, установку ПО сервера безопасности текущей версии следует выполнять на отдельных компьютерах. То есть для каждого сервера старой версии устанавливается сервер новой версии, в подчинение которому будут переходить обновляемые компьютеры. Это позволит до завершения обновления контролировать и оставшиеся компьютеры старой структуры, и обновленные компьютеры.

4. Установите компонент "Secret Net 7" на рабочем месте администратора безопасности.

5. Установите компонент "Secret Net 7 — Программа управления" на рабочем месте администратора безопасности.

> **Примечание:** Подробные сведения о процедурах модификации схемы Active Directory и установки компонентов см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".
>
> Для выполнения некоторых сценариев обновления необходимо иметь средства управления Secret Net (5.X или 6.X).

1. Подготовка установочного комплекта

Процедуру подготовки установочного комплекта необходимо выполнить отдельно для каждого сервера безопасности с размещением хранилища объектов ЦУ вне AD, если серверу будут подчинены компьютеры, ранее подчиненные серверу с хранилищем объектов ЦУ в AD.

1. Создайте папку, которая будет являться общедоступным сетевым ресурсом. В данной инструкции предлагается создать папку \Distrib на контроллере домена. Откройте общий доступ к этой папке. Дополнительно предоставьте права доступа к папке всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или для группы "Прошедшие проверку" ("Authenticated Users"). Необходимые права обеспечиваются установленными разрешениями на чтение, чтение и выполнение и просмотр содержимого.

> **Примечание:** Общедоступный сетевой ресурс можно создать на любом файловом сервере домена. Имя папки не регламентируется. Далее в инструкции в качестве общедоступного сетевого ресурса рассматривается папка \Distrib на контроллере домена.

2. Скопируйте в папку \Distrib содержимое установочного компакт-диска СЗИ Secret Net текущей версии, сохраняя структурную вложенность каталогов.

3. Перейдите в каталог \Tools\Infosec\AutoInstall.

4. В текстовом редакторе Блокнот откройте для редактирования файл SnInstall.Script и замените маску серийного номера на СНК текущей версии в строке: <SNSERIALNUMBER>XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX</SNSERIALNUMBER>.

> **Примечание:** Указанный файл содержит типовой сценарий установки клиента СЗИ Secret Net. Сценарий позволяет частично или полностью автоматизировать ввод информации, запрашиваемой программой установки клиента. Сведения о возможностях использования сценариев установки см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

5. С помощью файла MigrateToLds.vbs выполните модификацию программ установки СЗИ Secret Net. Для этого запустите консоль командной строки cmd.exe, перейдите в каталог \Distrib\Tools\Infosec\AutoInstall и введите команду: MigrateToLds.vbs <*имя_сервера_безопасности*> (в параметре укажите DNS-имя компьютера, который будет функционировать в качестве сервера безопасности).

2. Обновление и установка клиентов СЗИ Secret Net

2.1. Обновление или установка клиента на отдельном компьютере вручную с подчинением серверу безопасности и с переносом хранилища объектов ЦУ вне AD

1. На компьютере, где будет выполняться обновление или установка клиента, скопируйте содержимое папки \Distrib на локальный диск или подключите общедоступный сетевой ресурс как сетевой диск.

2. Запустите файл SnAutoRun.exe и в появившемся окне программы автозапуска выберите команду "Клиентское ПО".

3. Выполните обновление или установку ПО клиента в соответствии с описанием в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

4. Если выполнялось обновление клиента с версии 5.X или 6.X, запустите программу конфигурирования на рабочем месте администратора с установленными средствами управления соответствующей версии СЗИ Secret Net. В программе удалите из структуры оперативного управления компьютер, на котором было выполнено обновление.

5. На рабочем месте администратора безопасности запустите программу оперативного управления текущей версии в режиме конфигурирования. Добавьте компьютер в структуру ОУ с подчинением серверу безопасности в качестве клиента текущей версии.

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

2.2. Автоматическое обновление или установка клиентов

1. На рабочем месте администратора безопасности с установленной программой оперативного управления текущей версии запустите программу в режиме конфигурирования. Убедитесь в том, что на сервере безопасности зарегистрировано достаточное число лицензий для запланированного количества клиентов — для этого выберите сервер и перейдите на вкладку "Лицензии". При необходимости зарегистрируйте дополнительные серийные номера.

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

2. Создайте в доменах безопасности организационные подразделения для группирования компьютеров, на которых необходимо обновить или установить клиентское ПО. Для этого на компьютере контроллера домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — откройте оснастку "Управление групповой политикой", выберите последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup";

- в ОС Windows Server 2003 — откройте оснастку "Active Directory — пользователи и компьютеры", выберите последовательно каждый контейнер, которому сопоставлен домен безопасности (весь домен Active Directory или отдельное организационное подразделение), и активируйте команду меню "Действие | Создать | Подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autosetup".

Примечание:

Редактирование объектов Active Directory возможно на любом компьютере домена с установленными средствами централизованного управления ОС Windows. На контроллере домена такие средства установлены по умолчанию. Далее в инструкции в качестве компьютера с установленными средствами централизованного управления ОС Windows рассматривается контроллер домена.

Имя организационного подразделения не регламентируется. Далее в инструкции рассматривается организационное подразделение с именем "Secret Net Autosetup".

3. Создайте групповые политики автоматической установки для подразделения (подразделений) "Secret Net Autosetup". Политики создаются отдельно для применения на 32- и 64-разрядных версиях ОС Windows. Для создания политик на контроллере домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" выберите последовательно каждое подразделение "Secret Net Autosetup" и создайте политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды меню "Действие | Создать объект групповой политики в этом домене и связать его" (вариант англоязычного названия: "Create a GPO in this domain, and Link it here");
- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" последовательно вызовите диалоговое окно настройки свойств каждого подразделения "Secret Net Autosetup", перейдите на вкладку "Групповая политика" и создайте политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью кнопки "Создать".

Примечание: Имена групповых политик не регламентируются. Далее в инструкции рассматриваются групповые политики с именами "SNAutosetup Policy Win32" и "SNAutosetup Policy x64".

4. Настройте параметры выполнения сценариев групповых политик. Для этого на контроллере домена выполните следующие действия:

- В ОС Windows Server 2012/2008:

  1. В оснастке "Управление групповой политикой" последовательно выберите созданные политики (являются подчиненными объектами в организационных подразделениях "Secret Net Autosetup") и вызовите для каждой из них окно редактора групповых политик с помощью команды меню "Действие | Изменить".

  2. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Политики\Административные шаблоны:…\Система\Сценарии". Вызовите диалоговое окно настройки свойств параметра "Указать максимальное время выполнения сценариев групповой политики" ("Specify maximum wait time for Group Policy scripts" для ОС Windows Server 2012 или "Maximum wait time for Group Policy scripts" для ОС Windows Server 2008), установите отметку в поле "Включено" и укажите значение "7200".

  3. Вызовите диалоговое окно настройки свойств параметра "Отображать команды сценариев завершения работы во время их выполнения" ("Display instructions in shutdown scripts as they run") для ОС Windows Server 2012 или "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") для ОС Windows Server 2008 и установите отметку в поле "Включено".

- В ОС Windows Server 2003:

  1. В оснастке "Active Directory — пользователи и компьютеры" последовательно вызовите диалоговое окно настройки свойств каждого подразделения "Secret Net Autosetup" и перейдите на вкладку "Групповая политика".

  2. Последовательно выберите в списке каждую созданную политику и вызовите для нее окно редактора групповых политик с помощью кнопки "Изменить".

  3. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Административные шаблоны\Система\Сценарии". Вызовите диалоговое окно настройки свойств параметра "Maximum wait time for Group Policy scripts", установите отметку в поле "Включен" и укажите значение "7200".

  4. Вызовите диалоговое окно настройки свойств параметра "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") и установите отметку в поле "Включен".

5. В созданные групповые политики добавьте сценарии завершения работы. Для этого в окне редактора групповых политик (открытом на предыдущем действии) выполните следующие действия:

- В ОС Windows Server 2012/2008:

  1. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Политики\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".

  2. Добавьте сценарий с помощью кнопки "Добавить". В появившемся диалоге укажите следующие значения:

  - В поле "Имя сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>\auto_update74.cmd
    где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" укажите подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64.
  - В поле "Параметры сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>
    где необходимо указать тот же подкаталог, что и в поле "Имя сценария".

- В ОС Windows Server 2003:

  1. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".

  2. Добавьте сценарий с помощью кнопки "Добавить". В появившемся диалоге укажите следующие значения:

  - В поле "Имя сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>\auto_update74.cmd
    где в качестве подкаталога необходимо указать папку размещения дистрибутивных файлов соответствующей разрядности: для политики "SNAutosetup Policy Win32" укажите подкаталог \Win32, а для политики "SNAutosetup Policy x64" — подкаталог \x64.
  - В поле "Параметры сценария":
    \\<*имя_контроллера_домена*>\Distrib\Setup\Client\<*подкаталог*>
    где необходимо указать тот же подкаталог, что и в поле "Имя сценария".

6. Для всех выбранных к установке компьютеров, для которых будет выполняться обновление с версии СЗИ Secret Net 5.X или 6.X на текущую, на рабочем месте администратора безопасности запустите программу конфигурирования соответствующей версии и удалите компьютеры из структуры оперативного управления.

7. Запустите программу оперативного управления текущей версии в режиме конфигурирования и затем добавьте с подчинением серверу безопасности в качестве клиентов текущей версии ранее удаленные компьютеры, на которых будет проведено обновление, и новые компьютеры, на которых будет выполнена новая установка СЗИ Secret Net текущей версии.

8. Переместите в подразделение (подразделения) "Secret Net Autosetup" те компьютеры, на которых необходимо обновить или установить клиентское ПО. Перемещение компьютеров из других контейнеров выполняется в оснастке "Active Directory — пользователи и компьютеры" методом "Drag-and-Drop" или с помощью команды "Переместить" в контекстном меню компьютеров.

> **Пояснение:** Механизм автоматического обновления или установки ПО клиента начинает действовать на компьютерах после обновления групповых политик и перезагрузки этих компьютеров. Применение заданных групповых политик осуществляется на компьютерах автоматически в соответствии с установленным режимом обновления политик. Чтобы немедленно применить групповые политики на отдельном компьютере, используйте стандартные средства (например, локальную утилиту gpupdate).

9. На рабочем месте администратора безопасности запустите программу оперативного управления в режиме мониторинга. Используйте программу для контроля процесса установки ПО на компьютерах. После успешной установки и перезагрузки компьютеров соответствующие объекты структуры оперативного управления изменяют свое состояние. В частности, изменяются пиктограммы объектов и признаки состояния.

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

10. После того как обновление и установка клиентского ПО текущей версии произошли на всех компьютерах организационного подразделения "Secret Net Autosetup", переместите эти компьютеры обратно в исходные контейнеры в оснастке "Active Directory — пользователи и компьютеры".

11. После завершения обновления и установки клиентского ПО текущей версии на всех предусмотренных компьютерах удалите объекты, созданные для обеспечения автоматической установки:

1. На контроллере домена удалите папку \Distrib.

2. Удалите организационное подразделение "Secret Net Autosetup" и созданные групповые политики автоматической установки (после перемещения в исходные контейнеры всех компьютеров из этого подразделения). Для этого на контроллере домена выполните следующие действия:

- в ОС Windows Server 2012/2008 — в оснастке "Управление групповой политикой" перейдите к разделу "Объекты групповой политики" в иерархии объектов домена и удалите политики "SNAutosetup Policy Win32" и "SNAutosetup Policy x64" с помощью команды контекстного меню "Удалить". Затем аналогичным образом удалите организационное подразделение "Secret Net Autosetup";
- в ОС Windows Server 2003 — в оснастке "Active Directory — пользователи и компьютеры" удалите организационное подразделение "Secret Net Autosetup" с помощью команды контекстного меню "Удалить".