

Средство защиты информации Secret Net 6.5

Инструкция для автоматической установки клиентского ПО

Данный документ содержит развернутое описание последовательности действий для выполнения и контроля автоматической установки компонента "Secret Net 6" (клиент) на компьютерах.

1. На всех компьютерах системы, где будет установлено программное обеспечение СЗИ Secret Net 6, 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. Используя установочный компакт-диск СЗИ Secret Net 6, выполните следующие действия:
 1. Модифицируйте схему Active Directory.
 2. Установите компонент "Secret Net 6 — Сервер безопасности" на компьютерах, которые будут функционировать в качестве серверов безопасности.
 3. Установите компонент "Secret Net 6" на контроллере домена и APM администратора безопасности.
 4. Установите компонент "Secret Net 6 — Средства управления" на APM администратора безопасности.

Примечание: Подробные сведения о процедурах модификации схемы Active Directory и установки компонентов см. в документе "Средство защиты информации Secret Net 6. Установка, обновление и удаление. Руководство администратора".

3. Создайте папку, которая будет являться общедоступным сетевым ресурсом. В данной инструкции предлагается создать папку \Distrib на контроллере домена. Откройте общий доступ к этой папке.

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.

4. С установочного компакт-диска СЗИ Secret Net 6 скопируйте в папку \Distrib содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft. Если в системе имеются компьютеры, на которых будет использоваться средство аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card, дополнительно скопируйте в папку \Distrib содержимое каталога \Setup\SnTmCard.

5. Создайте файл со сценарием установки, используя доменный компьютер, на котором не установлено клиентское ПО системы Secret Net. Для создания файла сценария войдите в систему с правами локального администратора компьютера и выполните следующие действия:

1. На локальном диске создайте папку C:\ClientSN и с установочного компакт-диска СЗИ Secret Net 6 скопируйте в эту папку содержимое следующих каталогов (сохраняя их структурную вложенность): \Setup\Client и \Tools\Microsoft.

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

2. Запустите консоль командной строки (cmd.exe).
3. Введите команду для запуска программы установки в режиме создания файла сценария:
 - на компьютере под управлением 32-разрядной версии Windows:
start C:\ClientSN\Setup\Client\Win32\Setup.exe /script:3
 - на компьютере под управлением 64-разрядной версии Windows:
start C:\ClientSN\Setup\Client\x64\Setup.exe /script:3
4. В программе установки выполните требуемые действия до появления на экране диалога "Готова к установке программы", после чего отмените дальнейшую установку.
5. Убедитесь, что файл сценария SnInstall.script добавлен в каталог размещения дистрибутивных файлов (соответственно C:\ClientSN\Setup\Client\Win32 или C:\ClientSN\Setup\Client\x64).

Примечание: Подробные сведения о создании и редактировании файла со сценарием установки см. в документе "Средство защиты информации Secret Net 6. Установка, обновление и удаление. Руководство администратора".

6. Откройте созданный файл SnInstall.script в текстовом редакторе Блокнот и удалите значения параметров SNADMANAGERACCOUNTNAME и SNADMANAGERPASSWORD (если значения присутствуют). Строки с указанными параметрами должны выглядеть следующим образом:

```
<SNADMANAGERACCOUNTNAME></SNADMANAGERACCOUNTNAME>  
<SNADMANAGERPASSWORD></SNADMANAGERPASSWORD>
```

7. Скопируйте файл SnInstall.script в подкаталоги \Setup\Client\Win32 и \Setup\Client\x64 общедоступной папки \Distrib на контроллере домена. После копирования файла можно удалить папку C:\ClientSN на компьютере, который использовался для создания файла сценария.

8. На АРМ администратора безопасности запустите программу конфигурирования, активировав в главном меню Windows команду "Пуск | Все программы | Код безопасности | Secret Net | Консоль управления". Убедитесь в том, что на сервере безопасности зарегистрировано достаточное число лицензий для запланированного количества клиентов — для этого выберите сервер и перейдите к диалогу "Лицензии". При необходимости зарегистрируйте дополнительные серийные номера.

Примечание: Подробные сведения о работе с программой конфигурирования см. в документе "Средство защиты информации Secret Net 6. Конфигурирование. Руководство администратора".

9. Сформируйте в программе конфигурирования структуру оперативного управления — подчините серверу безопасности все компьютеры, на которых будет выполняться автоматическая установка клиента Secret Net 6. Для этого выполните следующие действия:

- 1.** В дереве структуры выберите папку "Свободные РС" нужного домена, активируйте команду "Действия | Добавить свободную рабочую станцию" и выберите компьютеры в стандартном диалоге выбора объектов ОС Windows. После добавления объекты появятся в папке "Свободные РС".
- 2.** В дереве структуры выберите сервер безопасности, отметьте нужные компьютеры в окне "Палитра объектов" и нажмите кнопку "Добавить" на панели инструментов в верхней части этого окна. Объекты будут перемещены в папку "Управляемые РС" выбранного сервера безопасности.

10. На контроллере домена откройте оснастку "Active Directory — пользователи и компьютеры" и выберите в дереве объектов домен, в котором необходимо настроить автоматическую установку.

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.

11. Создайте в домене организационное подразделение для автоматической установки ПО. Для этого выполните следующие действия:

- если контроллером домена является компьютер под управлением ОС Windows 2008 — активируйте команду меню "Action | New | Organizational Unit". В появившемся диалоге введите имя организационного подразделения "Secret Net Autoseup" и удалите отметку в поле "Protect container from accidental deletion" (названия элементов управления приведены для нерусифицированной версии ОС);
- если контроллером домена является компьютер под управлением ОС Windows 2000/2003 — активируйте команду меню "Действие | Создать | Подразделение". В появившемся диалоге введите имя организационного подразделения "Secret Net Autoseup" (названия элементов управления приведены для русифицированной версии ОС).

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

12. Переместите в подразделение "Secret Net Autoseup" те компьютеры, на которых необходимо выполнить автоматическую установку ПО на данном этапе. Перемещение компьютеров из контейнера или другого подразделения можно выполнять, например, методом "Drag-and-Drop" или с помощью команды "Переместить" в контекстном меню компьютеров.

Пояснение: Компьютеры необходимо переместить в организационное подразделение "Secret Net Autoseup" на время автоматической установки. После того, как программное обеспечение будет установлено, компьютеры следует вернуть в исходные контейнеры или организационные подразделения.

13. Создайте групповые политики автоматической установки для организационного подразделения "Secret Net Autoseup". 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 2008 — откройте оснастку "Group Policy Management", выберите организационное подразделение "Secret Net Autoseup" и создайте политики "SNAutoseup Policy Win32" и "SNAutoseup Policy x64" с помощью команды меню "Action | Create a GPO in this domain, and Link it here";
- в ОС Windows 2000/2003 — откройте оснастку "Active Directory — пользователи и компьютеры", вызовите диалоговое окно настройки свойств подразделения "Secret Net Autoseup", перейдите на вкладку "Групповая политика" и создайте политики "SNAutoseup Policy Win32" и "SNAutoseup Policy x64" с помощью кнопки "Создать".

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

14. В созданные групповые политики добавьте сценарии автозагрузки. Для этого на контроллере домена выполните следующие действия:

- В ОС Windows 2008:
 - 1.** В оснастке "Group Policy Management" выберите созданную политику (является подчиненным объектом организационного подразделения "Secret Net Autoseup") и вызовите для нее окно редактора групповых политик с помощью команды меню "Action | Edit".
 - 2.** В дереве объектов редактора перейдите к разделу "Computer Configuration\Policies\Windows Settings\Scripts" и вызовите диалоговое окно настройки свойств параметра "Startup".
 - 3.** Добавьте сценарий с помощью кнопки "Add". В поле "Script Parameters" введите значение "/autoinstall" (без кавычек). В поле "Script Name" введите:
 - для политики "SNAutoseup Policy Win32":
\\<имя_контроллера_домена>\Distrib\Setup\Client\Win32\Setup.exe
 - для политики "SNAutoseup Policy x64":
\\<имя_контроллера_домена>\Distrib\Setup\Client\x64\Setup.exe
 - 4.** Аналогично выполните действия **1–3** для второй политики.
- В ОС Windows 2000/2003:
 - 1.** В оснастке "Active Directory — пользователи и компьютеры" вызовите диалоговое окно настройки свойств подразделения "Secret Net Autoseup" и перейдите на вкладку "Групповая политика".
 - 2.** Выберите в списке созданную политику и вызовите для нее окно редактора групповых политик с помощью кнопки "Изменить".
 - 3.** В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Автозагрузка".
 - 4.** Добавьте сценарий с помощью кнопки "Добавить". В поле "Параметры сценария" введите значение "/autoinstall" (без кавычек). В поле "Имя сценария" введите:
 - для политики "SNAutoseup Policy Win32":
\\<имя_контроллера_домена>\Distrib\Setup\Client\Win32\Setup.exe
 - для политики "SNAutoseup Policy x64":
\\<имя_контроллера_домена>\Distrib\Setup\Client\x64\Setup.exe
 - 5.** Аналогично выполните действия **2–4** для второй политики.

15. Включите действие созданных групповых политик. Для этого на контроллере домена выполните следующие действия:

- В ОС Windows 2008:
 - 1.** В оснастке "Group Policy Management" выберите созданную политику (является подчиненным объектом организационного подразделения "Secret Net Autoseup") и вызовите для нее окно редактора групповых политик с помощью команды меню "Action | Edit".
 - 2.** В дереве объектов редактора перейдите к разделу "Computer Configuration\Policies\Administrative Templates...\System\Group Policy", вызовите диалоговое окно настройки свойств параметра "Scripts policy processing" и установите отметку в поле "Enabled". Дополнительно установите отметки в полях "Do not apply during periodic background processing" и "Process even if the Group Policy objects have not changed".
 - 3.** В дереве объектов редактора перейдите к разделу "Computer Configuration\Policies\Administrative Templates...\System\Logon", вызовите диалоговое окно настройки свойств параметра "Always wait for the network at computer startup and logon" и установите отметку в поле "Enabled".
 - 4.** В дереве объектов редактора перейдите к разделу "Computer Configuration\Policies\Administrative Templates...\System\Scripts", вызовите диалоговое окно настройки свойств параметра "Run startup scripts asynchronously" и установите отметку в поле "Disabled".
 - 5.** Аналогично выполните действия **1–4** для второй политики.
- В ОС Windows 2003:
 - 1.** В оснастке "Active Directory — пользователи и компьютеры" вызовите диалоговое окно настройки свойств подразделения "Secret Net Autoseup" и перейдите на вкладку "Групповая политика".
 - 2.** Выберите в списке 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\System\Group Policy", вызовите диалоговое окно настройки свойств параметра "Scripts policy processing" и установите отметку в поле "Включен". Дополнительно установите отметки в полях "Do not apply during periodic background processing" и "Process even if the Group Policy objects have not changed".
 4. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Административные шаблоны\System\Logon", вызовите диалоговое окно настройки свойств параметра "Always wait for the network at computer startup and logon" и установите отметку в поле "Включен".
 5. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Административные шаблоны\System\Scripts", вызовите диалоговое окно настройки свойств параметра "Run startup scripts asynchronously" и установите отметку в поле "Отключен".
 6. Аналогично выполните действия **2–5** для второй политики.
- В ОС Windows 2000:
 1. В оснастке "Active Directory — пользователи и компьютеры" вызовите диалоговое окно настройки свойств подразделения "Secret Net Autoseup" и перейдите на вкладку "Групповая политика".
 2. Выберите в списке 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\System\Group Policy", вызовите диалоговое окно настройки свойств параметра "Scripts policy processing" и установите отметку в поле "Включен". Дополнительно установите отметки в полях "Do not apply during periodic background processing" и "Process even if the Group Policy objects have not changed".
 4. В том же разделе вызовите диалоговое окно настройки свойств параметра "Apply Group Policy for computers asynchronously during startup" и установите отметку в поле "Отключен".
 5. В дереве объектов редактора перейдите к разделу "Конфигурация компьютера\Административные шаблоны\System\Logon", вызовите диалоговое окно настройки свойств параметра "Run startup scripts asynchronously" и установите отметку в поле "Отключен".
 6. Аналогично выполните действия **2–5** для второй политики.

Пояснение: Механизм автоматической установки ПО клиента начинает действовать на компьютерах после обновления групповых политик на этих компьютерах. 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 groupdate).

Автоматическая установка осуществляется на этапе загрузки компьютера до входа пользователя в систему, поэтому для запуска процесса установки пользователю необходимо перезагрузить компьютер. По завершении процесса установки автоматически происходит перезагрузка компьютера, после которой компьютер готов к работе.

16. На АРМ администратора безопасности запустите программу мониторинга, активировав в главном меню Windows команду "Пуск | Все программы | Код безопасности | Secret Net | Монитор". 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 мониторинга см. в документе "Средство защиты информации Secret Net 6. Мониторинг и оперативное управление. Руководство администратора".

17. После того, как установка ПО произошла на всех компьютерах организационного подразделения "Secret Net Autoseup", переместите эти компьютеры обратно в исходные контейнеры в оснастке "Active Directory — пользователи и компьютеры". Для выполнения автоматической установки на других компьютерах, поместите их в подразделение "Secret Net Autoseup".

18. После завершения автоматической установки ПО на всех предусмотренных компьютерах установите драйвер средства аппаратной поддержки Secret Net Card на тех компьютерах, на которых будет использоваться средство аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card. Установка драйвера выполняется локально. Для установки драйвера войдите в систему с правами локального администратора компьютера и введите команду запуска программы установки:

- на компьютере под управлением 32-разрядной версии Windows:
`"\<имя_контроллера_домена>\Distrib\Setup\SnTmCard\Win32\Драйвер платы Secret Net Touch Memory Card.msi"`
- на компьютере под управлением 64-разрядной версии Windows:
`"\<имя_контроллера_домена>\Distrib\Setup\SnTmCard\x64\Драйвер платы Secret Net Touch Memory Card.msi"`

19. Удалите объекты, созданные для обеспечения автоматической установки:

- 1.** На контроллере домена удалите папку \Distrib.
- 2.** Удалите организационное подразделение "Secret Net Autoseup" 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 2008 — в оснастке "Group Policy Management" перейдите к разделу "Group Policy Objects" в иерархии объектов домена и удалите политики "SNAutoseup Policy Win32" и "SNAutoseup Policy x64" с помощью команды контекстного меню "Delete". Затем аналогичным образом удалите организационное подразделение "Secret Net Autoseup".
 - в ОС Windows 2000/2003 — в оснастке "Active Directory — пользователи и компьютеры" удалите организационное подразделение "Secret Net Autoseup" с помощью команды контекстного меню "Удалить".