Средство защиты информации Secret Net
Инструкция по локальному обновлению клиента Secret Net

Данный документ содержит развернутое описание последовательности действий для локального обновления клиента СЗИ Secret Net на версию 7.6 (далее — новая версия). Рассматриваются варианты обновления клиента в автономном и сетевом режимах функционирования.

Примечание: В системе Secret Net предусмотрены возможности автоматической установки и обновления клиента в сетевом режиме функционирования. Описание действий для настройки автоматической установки и обновления приводится в документах:

"Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

"Инструкция по автоматической установке клиента Secret Net 7" — содержит развернутое описание последовательности действий для случаев обновления клиентов, если после обновления компьютеры будут подчинены серверу безопасности с таким же размещением хранилища объектов централизованного управления (или в Active Directory, или вне AD).

"Инструкция по обновлению на Secret Net 7" — содержит развернутое описание последовательности действий для обновления клиентов на компьютерах, подчиненных серверу безопасности с размещением хранилища объектов ЦУ в AD, с последующим подчинением этих компьютеров серверу безопасности с размещением хранилища объектов ЦУ вне AD.

Процедуры обновления рассматриваются на примере обновления клиента Secret Net версии 5.0. Обновление клиентов других версий выполняется аналогично.

1. Обновление клиента в автономном режиме

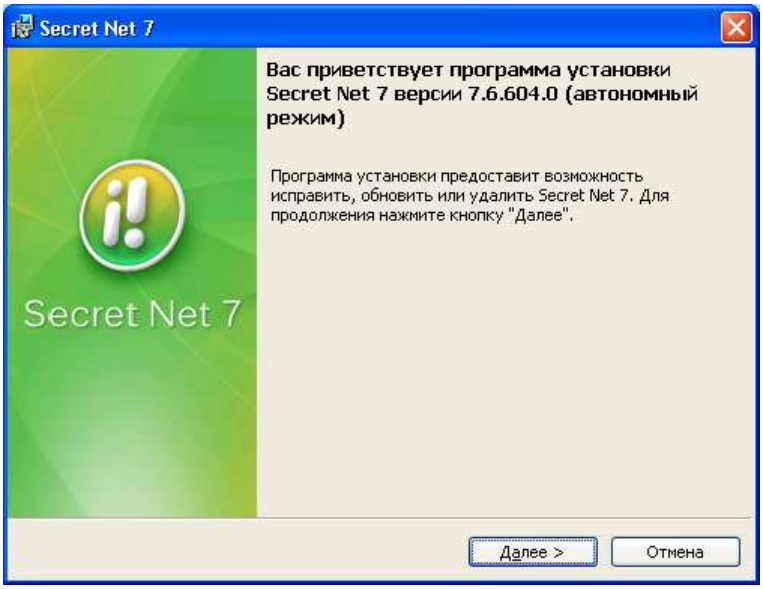
Перед обновлением выполните следующие подготовительные действия:

- если на компьютере имеются файлы, зашифрованные средствами СЗИ Secret Net предыдущей версии, перед обновлением обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен;
- если в СЗИ Secret Net версии 5.X включен режим усиленной аутентификации и используются идентификаторы eToken, отключите режим усиленной аутентификации по ключу.

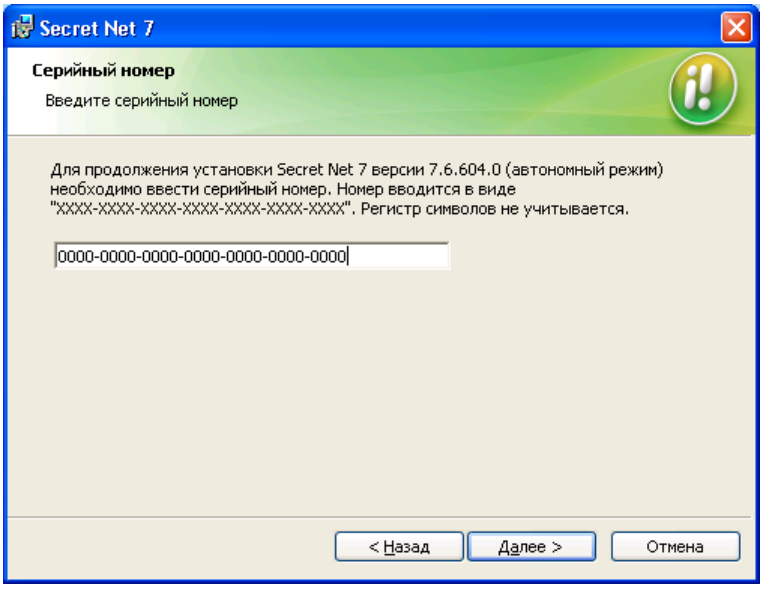
1. Войдите в систему с учетными данными администратора.

2. Вставьте в привод установочный диск системы Secret Net новой версии. Дождитесь появления окна программы автозапуска:

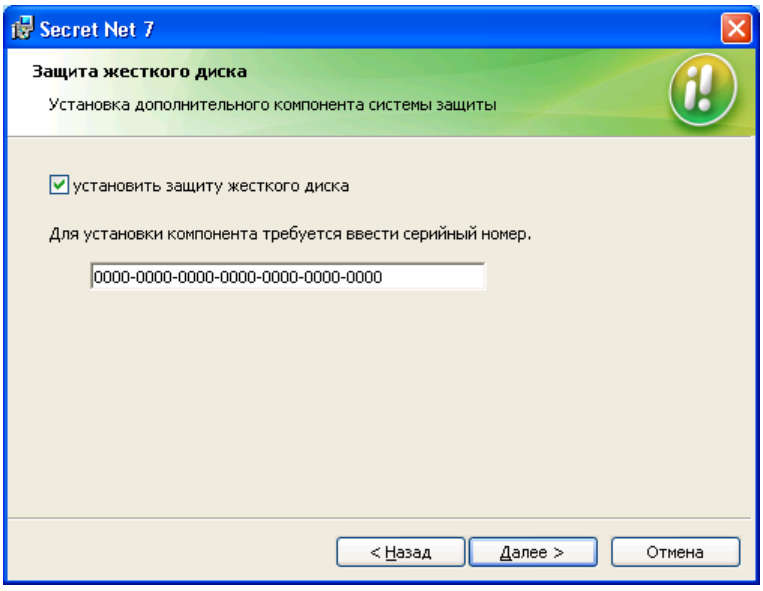
3. Запустите обновление с помощью команды "Клиентское ПО". После запуска программы установки закройте окно программы автозапуска. Дождитесь завершения подготовительных действий программы установки, по окончании которых на экран будет выведен диалог приветствия:



4. Нажмите кнопку "Далее >". На экране появится диалог "Серийный номер":

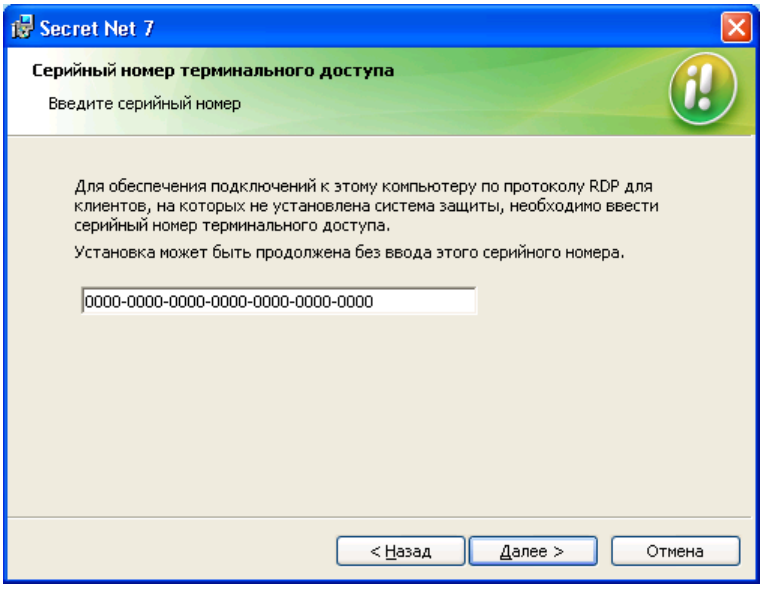


5. Введите серийный номер клиента для автономного режима функционирования и нажмите кнопку "Далее >". На экране появится диалог "Защита жесткого диска" (в случае, если на компьютере не зарегистрирован серийный номер подсистемы защиты дисков):

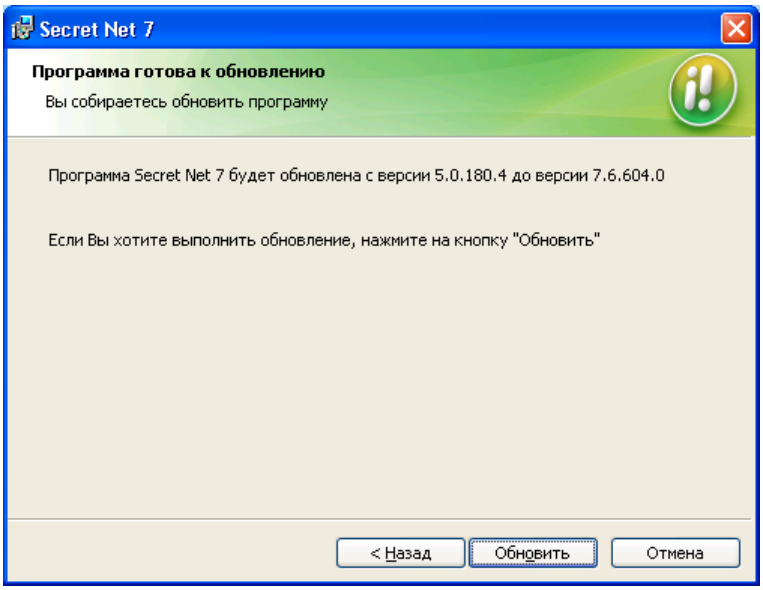


6. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма. Если механизм не будет использоваться, оставьте поле неотмеченным. Для продолже-

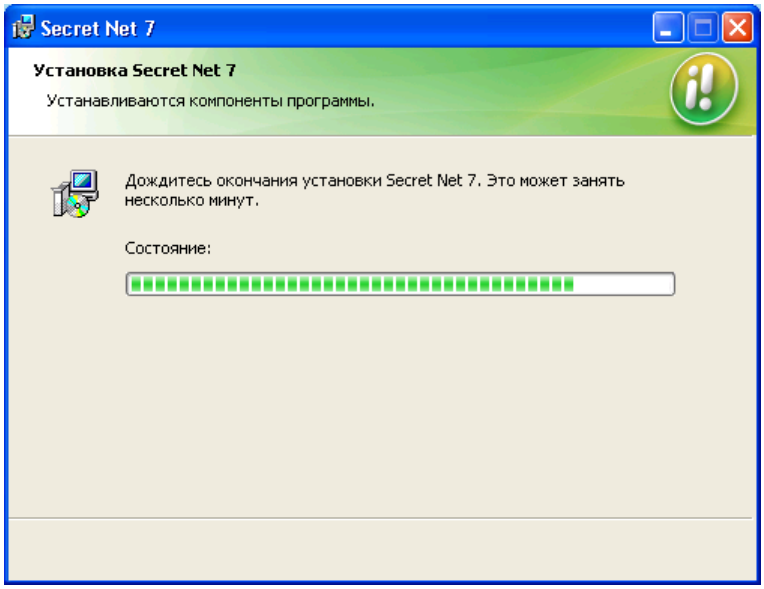
ния установки нажмите кнопку "Далее >". На экране появится диалог "Серийный номер терминального доступа" (при обновлении с версии до 7.2, а также в случае, если на компьютере зарегистрирован неподходящий серийный номер разрешения терминальных подключений):



7. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера. Для продолжения установки нажмите кнопку "Далее >". Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению":



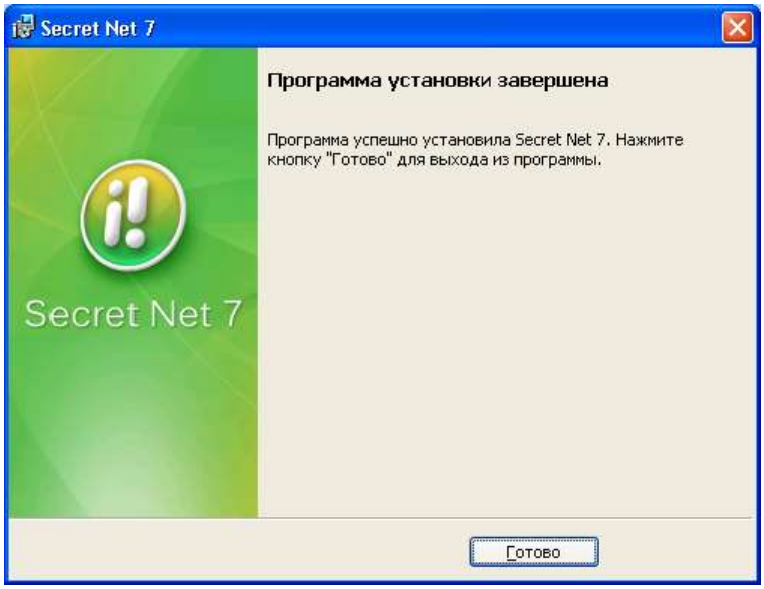
8. Нажмите кнопку "Обновить". Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса:



Примечание: В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующих случаях:

- Если не завершена работа программы автозапуска (см. действие **3**), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

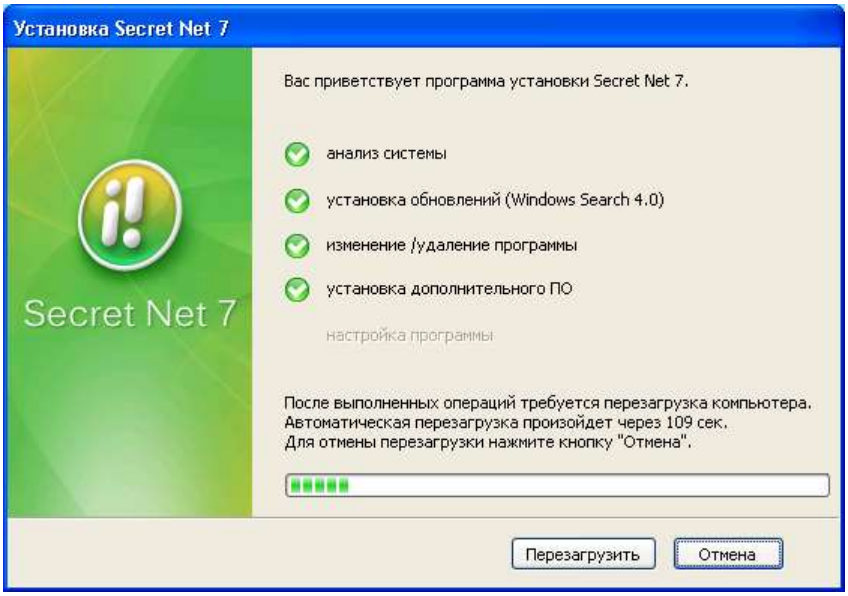
По окончании обновления появится диалог "Программа установки завершена":



9. Проверьте состав подключенных к компьютеру устройств. Если подключены устройства, которые в дальнейшем должны быть запрещены к использованию, — отключите их.

Примечание: При первой загрузке компьютера после установки ПО системы Secret Net текущая аппаратная конфигурация автоматически принимается в качестве эталонной. Поэтому до перезагрузки необходимо отключить те устройства, которые должны быть запрещены к использованию на данном компьютере.

10. В диалоге "Программа установки завершена" нажмите кнопку "Готово". На экране появится завершающий диалог программы установки:



11. Нажмите кнопку "Перезагрузить" (кнопка появляется после выполнения всех операций в списке) и дождитесь окончания перезагрузки компьютера.

12. На компьютере под управлением ОС Windows XP/2003 при необходимости использования идентификаторов eToken удалите ПО eToken Run Time Environment и установите ПО eToken PKI Client. Комплект для установки размещается на установочном диске системы Secret Net новой версии в каталоге \Tools\eToken\PKI Client 5.1.

Примечание: В новой версии не поддерживаются идентификаторы eToken R2.

2. Обновление клиента в сетевом режиме

Обновление клиента в сетевом режиме функционирования осуществляется в следующем порядке:

1. Подчинение компьютера серверу безопасности новой версии.

2. Обновление ПО клиента на защищаемом компьютере.

3. Локальное конфигурирование клиента для работы в структуре ОУ. Данная процедура выполняется в случае, если компьютер был подчинен серверу безопасности с размещением хранилища объектов централизованного управления в Active Directory, а после обновления подчиняется серверу с размещением хранилища объектов ЦУ вне AD.

2.1. Подчинение компьютера серверу безопасности новой версии

Подчинение компьютера с установленным клиентом версии 7.2 и выше серверу безопасности новой версии происходит автоматически при обновлении ПО сервера безопасности предыдущей версии (того сервера, которому компьютер был подчинен до обновления).

Если на компьютере установлен клиент до версии 7.2 (5.X, 6.X), необходимо переподчинить компьютер серверу безопасности новой версии. Действия для переподчинения выполняются администратором с правами на конфигурирование структуры ОУ с помощью средств управления СЗИ Secret Net обновляемой и новой версий. Для этого в системе должны быть представлены следующие компоненты СЗИ:

- сервер безопасности предыдущей версии (которому подчинен компьютер);
- средства управления для подключения к серверу безопасности предыдущей версии;
- сервер безопасности новой версии (которому будет подчинен компьютер);
- программа оперативного управления для подключения к серверу новой версии.

Примечание: Описание порядка установки компонентов новой версии приводится в документе "Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление".

Для переподчинения компьютера администратору необходимо выполнить следующие действия:

1. На рабочем месте с установленными средствами управления предыдущей версии СЗИ Secret Net запустить программу конфигурирования (в версиях СЗИ 5.X или 6.X) или программу оперативного управления в режиме конфигурирования (в остальных версиях) с подключением к серверу безопасности предыдущей версии. В программе удалить из структуры оперативного управления компьютер, на котором будет выполняться локальное обновление.

2. На рабочем месте с установленной программой оперативного управления новой версии запустить программу в режиме конфигурирования с подключением к серверу безопасности новой версии. Добавить компьютер в структуру ОУ с подчинением серверу безопасности в качестве клиента новой версии. Затем на вкладке "Лицензии" добавить нужные серийные номера лицензий и сохранить изменения.

2.2. Обновление клиента на компьютере

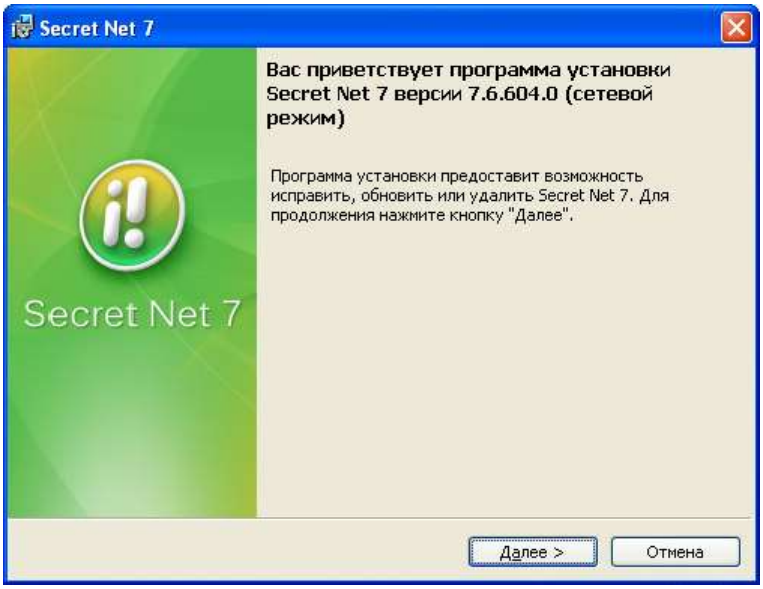
Перед обновлением выполните следующие подготовительные действия:

- если на компьютере имеются файлы, зашифрованные средствами СЗИ Secret Net предыдущей версии, перед обновлением обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен;
- если в СЗИ Secret Net версии 5.X включен режим усиленной аутентификации и используются идентификаторы eToken, отключите режим усиленной аутентификации по ключу.

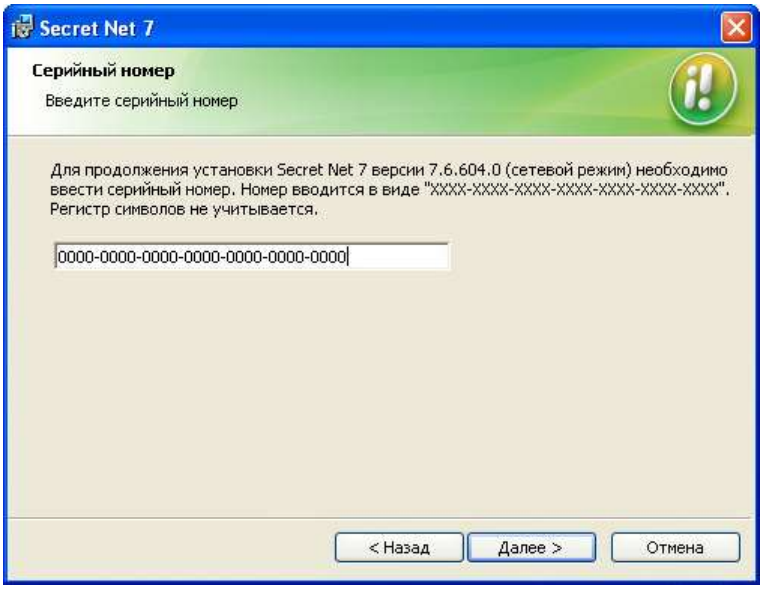
1. Войдите в систему с учетными данными администратора.

2. Вставьте в привод установочный диск системы Secret Net новой версии. Дождитесь появления окна программы автозапуска:

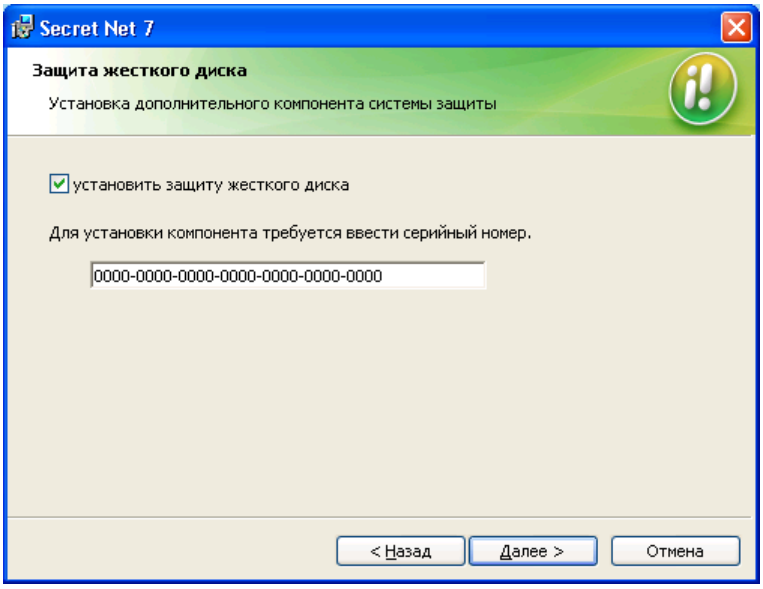
3. Запустите обновление с помощью команды "Клиентское ПО". После запуска программы установки закройте окно программы автозапуска. Дождитесь завершения подготовительных действий программы установки, по окончании которых на экран будет выведен диалог приветствия:



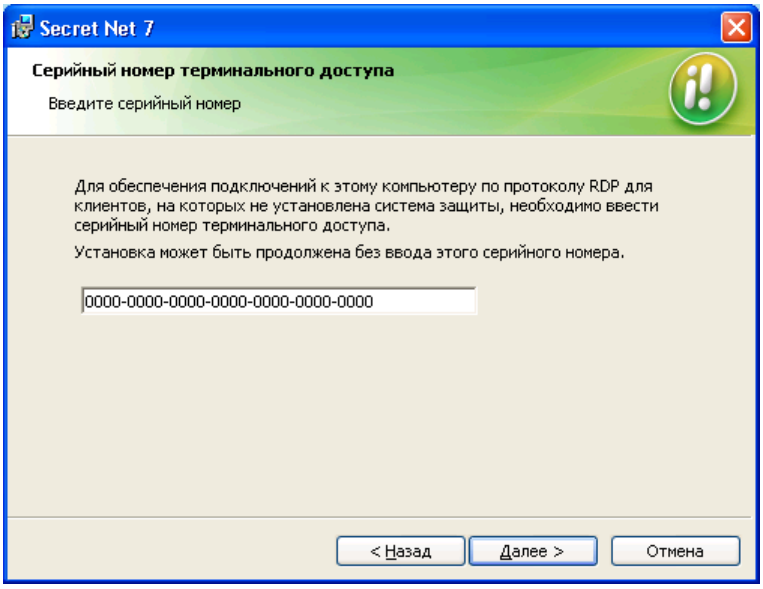
4. Нажмите кнопку "Далее >". На экране появится диалог "Серийный номер":



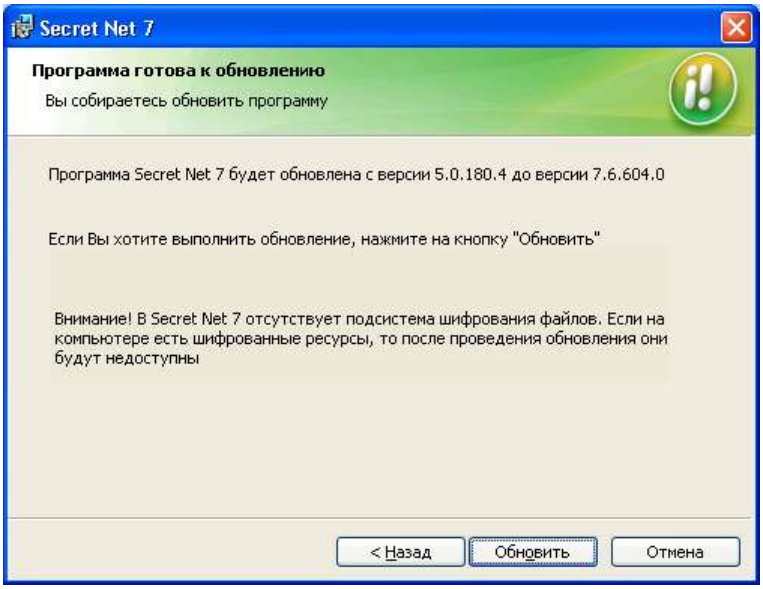
5. Введите серийный номер клиента для сетевого режима функционирования и нажмите кнопку "Далее >". На экране появится диалог "Защита жесткого диска" (в случае, если на компьютере не зарегистрирован серийный номер подсистемы защиты дисков):



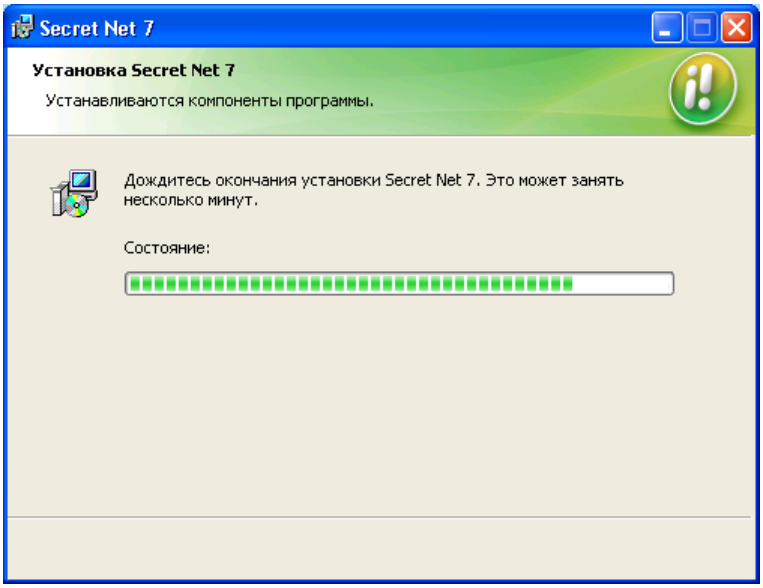
6. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма. Если механизм не будет использоваться, оставьте поле неотмеченным. Для продолжения установки нажмите кнопку "Далее >". На экране появится диалог "Серийный номер терминального доступа" (при обновлении с версии до 7.2, а также в случае, если на компьютере зарегистрирован неподходящий серийный номер разрешения терминальных подключений):



7. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера. Для продолжения установки нажмите кнопку "Далее >". Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению":



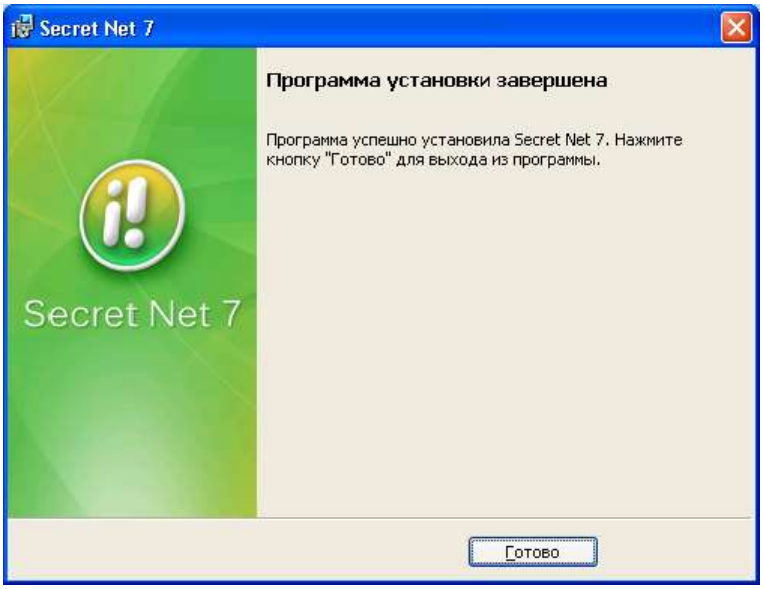
8. Нажмите кнопку "Обновить". Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса:



Примечание: В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующих случаях:

- Если не завершена работа программы автозапуска (см. действие **3**), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

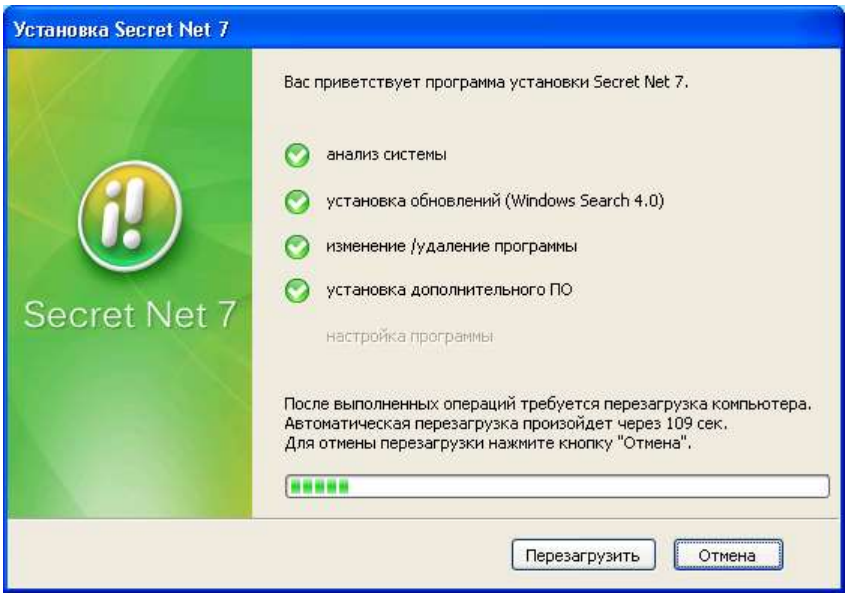
По окончании обновления появится диалог "Программа установки завершена":



9. Проверьте состав подключенных к компьютеру устройств. Если подключены устройства, которые в дальнейшем должны быть запрещены к использованию, — отключите их.

Примечание: При первой загрузке компьютера после установки ПО системы Secret Net текущая аппаратная конфигурация автоматически принимается в качестве эталонной. Поэтому до перезагрузки необходимо отключить те устройства, которые должны быть запрещены к использованию на данном компьютере.

10. В диалоге "Программа установки завершена" нажмите кнопку "Готово". На экране появится завершающий диалог программы установки:



11. Нажмите кнопку "Перезагрузить" (кнопка появляется после выполнения всех операций в списке) и дождитесь окончания перезагрузки компьютера.

12. На компьютере под управлением ОС Windows XP/2003 при необходимости использования идентификаторов eToken удалите ПО eToken Run Time Environment и установите ПО eToken PKI Client. Комплект для установки размещается на установочном диске системы Secret Net новой версии в каталоге \Tools\eToken\PKI Client 5.1.

Примечание: В новой версии не поддерживаются идентификаторы eToken R2.

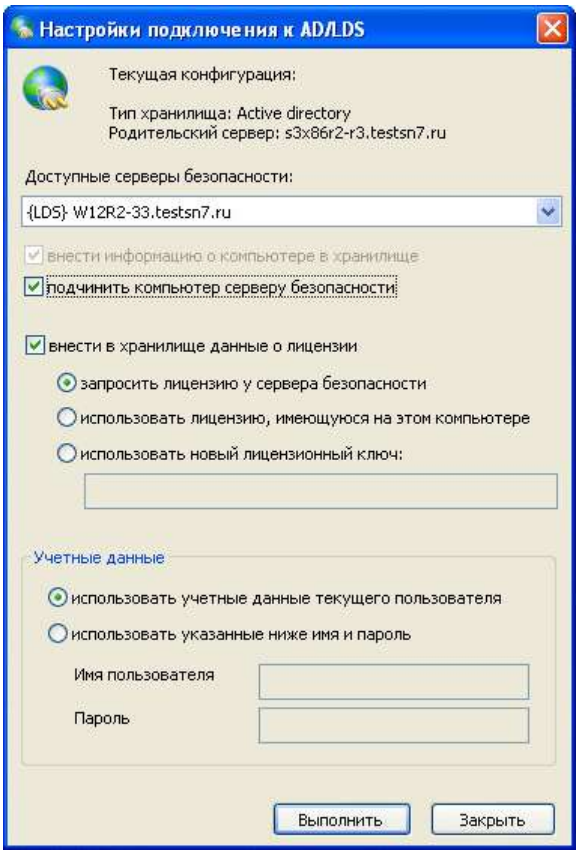
2.3. Локальное конфигурирование клиента для работы в структуре ОУ

Процедуру локального конфигурирования необходимо выполнить в следующем случае: если компьютер был подчинен серверу безопасности с размещением хранилища объектов централизованного управления в Active Directory, а после обновления подчиняется серверу с размещением хранилища объектов ЦУ вне AD. Процедура выполняется на компьютере локально с помощью специальной программы из состава клиентского ПО Secret Net новой версии.

1. Войдите в систему с учетными данными администратора.

2. Запустите стандартную оснастку управления локальными службами Windows (в разделе средств администрирования Панели управления) и остановите работу службы "Secret Net Agent".

3. Откройте каталог установки клиента и запустите на исполнение файл SnLDAPConfig.exe. На экране появится диалог программы локального конфигурирования клиента. После получения данных в диалоге появятся сведения о текущей конфигурации клиента и список доступных серверов безопасности:



4. В поле "Доступные серверы безопасности" выберите сервер безопасности новой версии и установите отметку в поле "подчинить компьютер серверу безопасности".

5. Нажмите кнопку "Выполнить". По окончании выполнения регистрационных действий на экране появится сообщение программы.

6. Нажмите кнопку "ОК" в окне сообщения, закройте программу и снова запустите службу "Secret Net Agent".