КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Сервер обновлений. Установка и настройка

© Компания "Код Безопасности", 2018. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для развертывания и настройки средства автоматического обновления антивирусных баз на рабочих станциях в локальной сети.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Архитектура сервера обновлений

ПО Secret Net Studio включает в себя серверы обновлений для Антивируса и Антивируса (технология ESET). Серверы обновлений предназначены для централизованного обновления баз антивирусов на защищаемых компьютерах. Загрузка обновлений производится с сервера компании "Код Безопасности".

Системные требования

Сервер обновлений может быть установлен на компьютеры под управлением следующих операционных систем:

- Windows Server 2008 x64 R2 SP1;
- Windows Server 2012/Server 2012 R2.

Сервер обновлений может быть использован только с сервером IIS версии 7 и выше.

Примечание. SSL-сертификат, устанавливаемый для сервера IIS, является самозаверенным.

Примечание. В Secret Net Studio 8.2 входящий сетевой трафик на локальных серверах обновлений состоит из пакетов обновлений и утилит обновления (см. стр. 13).

Варианты размещения

В зависимости от конфигурации и размера сети могут использоваться различные схемы размещения сервера обновлений.

Защищаемая сеть с малым числом рабочих станций

Этот вариант рекомендуется использовать, когда в сети не более 5 защищаемых компьютеров. В этом случае в программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с сервера компании "Код Безопасности" (см. документ "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Защищаемая сеть с большим числом рабочих станций

Этот вариант целесообразно использовать, если в сети более 5 защищаемых компьютеров. В этом случае нужно установить ПО сервера обновлений на выделенном сервере в защищаемой сети. Установленный сервер обновлений будет загружать обновления с сервера компании "Код Безопасности" и предоставлять обновления клиентам в сети и другим серверам обновлений, используемым в каскадном режиме (не расходуя внешний трафик). В программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с локального сервера (см. документ "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Защищаемая сеть не подключена к Интернету

В этом случае необходимо установить отдельный сервер, имеющий доступ к Интернету. На этом сервере нужно установить ПО сервера обновлений. На сервере в закрытой сети также нужно установить ПО сервера обновлений.

Сервер обновлений, имеющий доступ к Интернету, будет загружать обновления с сервера компании "Код Безопасности" и хранить их. Обновления с этого сервера на сервер в закрытой сети необходимо переносить вручную.

В программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить функцию обновления антивирусных баз с локаль-

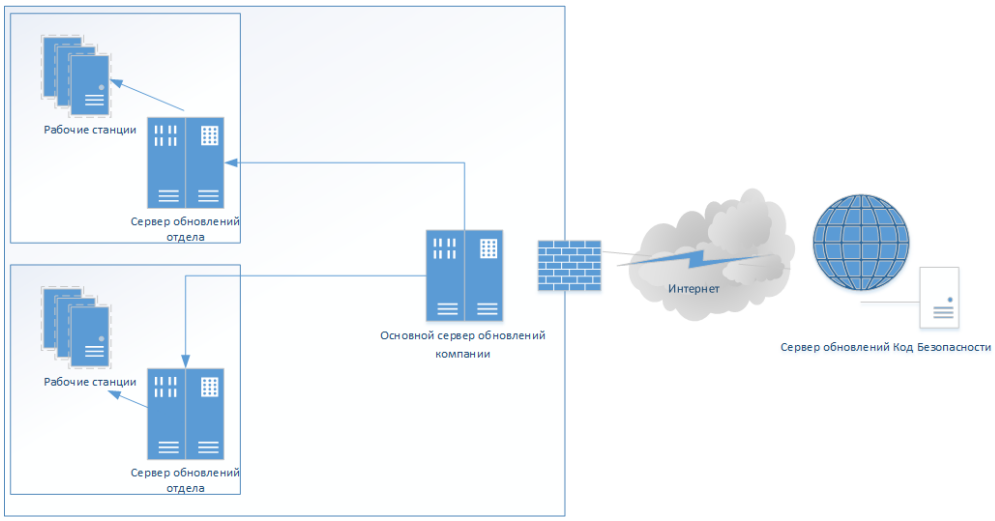
ного сервера в закрытой сети (см. документ "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Каскадирование серверов

Внутри компании создается каскад серверов, в котором один, корневой, скачивает обновления с сервера компании "Код Безопасности", а остальные, дочерние, скачивают обновления с корневого сервера обновлений или с других дочерних серверов.

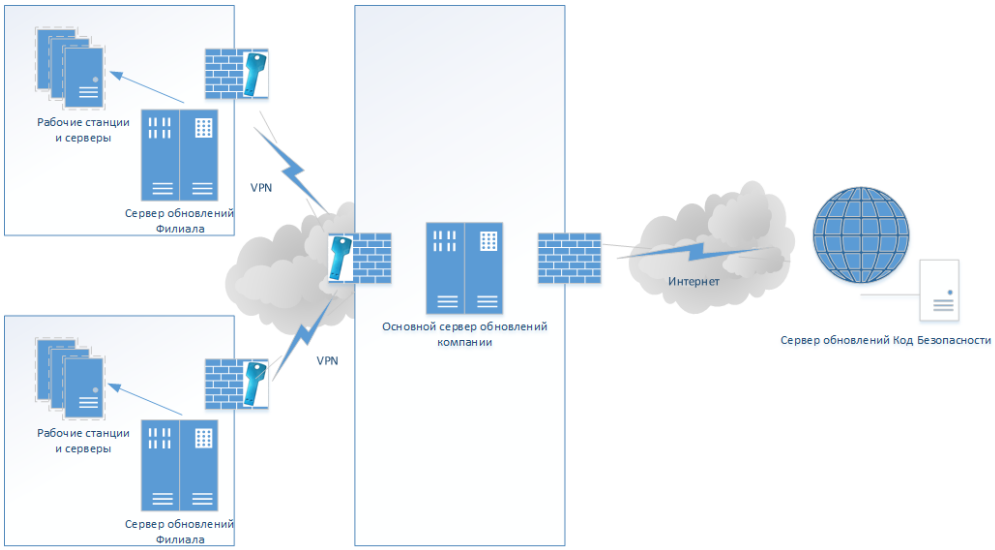
Пример 1. В компании используется несколько подсетей.

В этом случае устанавливается основной сервер обновлений, который загружает обновления с сайта компании "Код Безопасности". В каждой подсети устанавливается свой сервер обновлений, настроенный на загрузку обновлений с основного сервера. С этих серверов загружают обновления рабочие станции подсети.



Пример 2. В компании несколько филиалов.

В каждом филиале устанавливается сервер обновлений. Каждый сервер загружает обновления, доступные внутри головной организации, по корпоративной сети.



Глава 2
Установка и настройка сервера обновлений

Для развертывания сервера обновлений:

1. Выполните установку ПО Сервера обновлений Secret Net Studio (см. стр.**7**).
2. Настройте загрузку обновлений с сервера компании "Код Безопасности" (см. стр.**12**) или с локального сервера обновлений (см. стр.**12**).
3. Настройте расписание обновлений (см. стр.**13**).

Установка сервера обновлений

Установка сервера обновлений для Антивируса (технология ESET)

Для установки сервера обновлений:

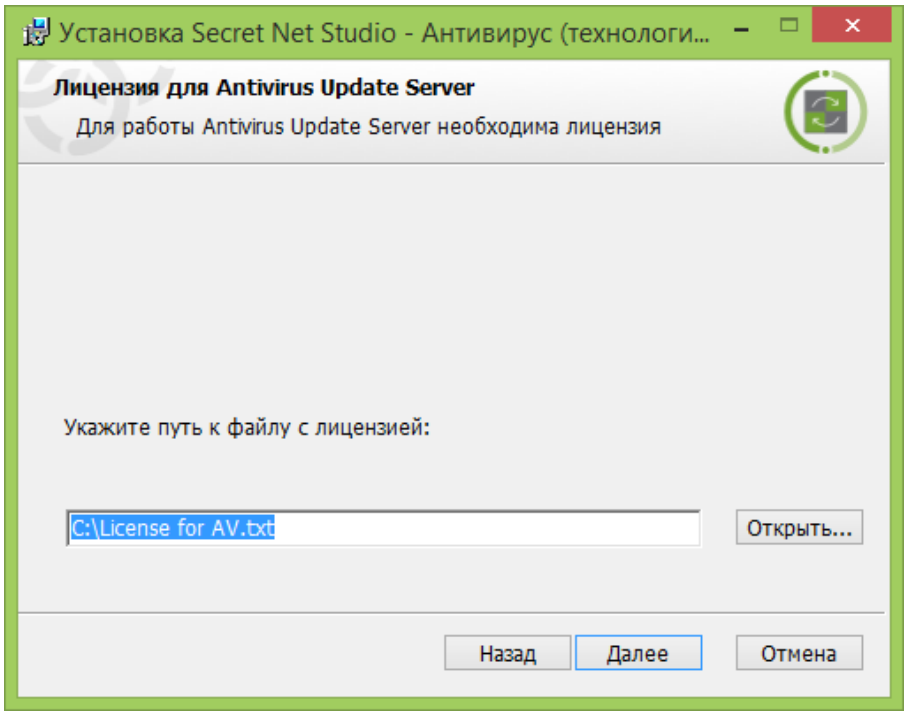
1. Войдите в систему с правами администратора компьютера.
2. Запустите на исполнение файл AvUpdateServer.msi от имени администратора.

   Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.
3. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
4. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

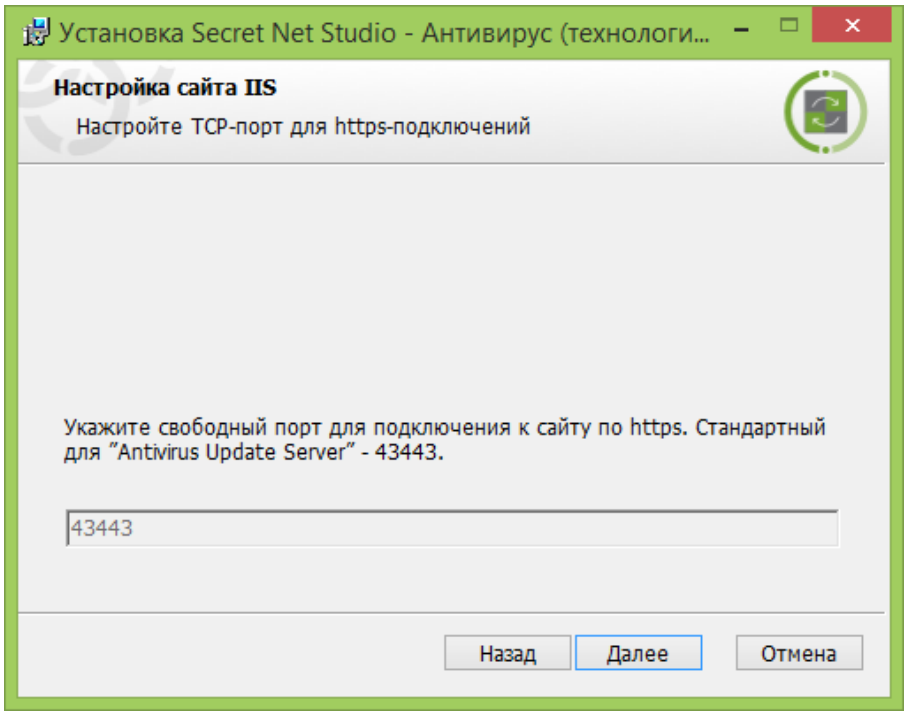
Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

5. На экране появится диалог.



Укажите путь к файлу с лицензией для сервера обновлений и нажмите "Далее".

6. На экране появится окно настройки порта для HTTPS-подключений.



По умолчанию используется порт 43443.

Нажмите кнопку "Далее". На экране появится диалог с сообщением о готовности к установке.

7. Нажмите кнопку "Установить".

Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемого компонента. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

После успешной установки и настройки компонента на экране появится диалог с сообщением об успешном завершении установки.

8. Нажмите кнопку "Готово".

Установка сервера обновлений для Антивируса

Для установки сервера обновлений:

1. Войдите в систему с правами администратора компьютера.
2. Запустите на исполнение файл AmUpdateServer.msi от имени администратора.

Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.

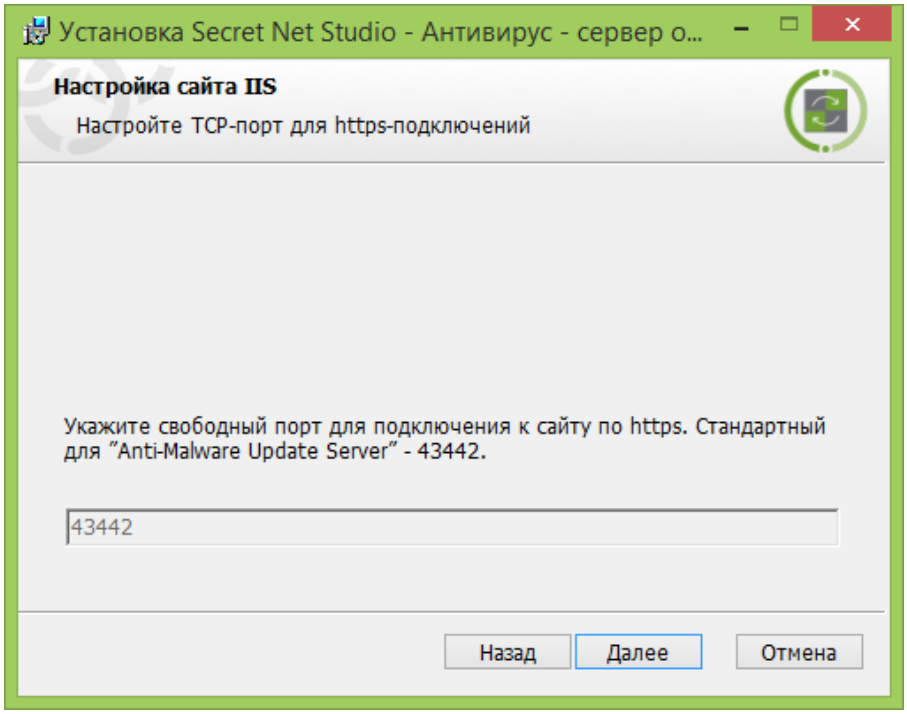
3. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

5. На экране появится окно настройки порта для HTTPS-подключений.



По умолчанию используется порт 43442.

Нажмите кнопку "Далее". На экране появится диалог с сообщением о готовности к установке.

6. Нажмите кнопку "Установить".

   Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемого компонента. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

   После успешной установки и настройки компонента на экране появится диалог с сообщением об успешном завершении установки.

7. Нажмите кнопку "Готово".

Настройка сервера обновлений

Установленный сервер обновлений для Антивируса (технология ESET) располагается в каталоге C:\Program Files (x86)\Security Code\Secret Net Studio\Server\Antivirus Update Server, для Антивируса в каталоге C:\Program Files (x86)\Security Code\Secret Net Studio\Server\Antimalware Update Server.

Для вызова подробной информации о программе откройте командную строку и введите следующую команду:

```
avus.exe
```

Примечание. Для изменения любых параметров с помощью утилиты avus.exe необходимо наличие прав администратора. Команды, не изменяющие настройки сервера обновлений, может выполнить любой пользователь.

Для настройки работы сервера обновлений используются следующие параметры.

Примечание. Утилита управления сервером обновлений avus.exe и утилита управления антивирусами на защищаемых компьютерах av_cli.exe используют одинаковые параметры для управления обновлениями.

Команда	Возможные аргументы	Действие
-c:list_update	**-package_id:** — номер пакета	Получить информацию о пакете обновлений
-c:list_update_job	**-update_job_id:** — номер задачи	Получить информацию о задаче
-c:list_update_jobs		Получить список существующих задач обновления
-c:list_updates		Получить список пакетов обновлений в системе
-c:new_update_job		Начать обновление
-c:new_update_rollback_job	**-package_id:** — номер обновления	Выполнить откат системы на обновление
-c:cancel_update_job	**-update_job_id:** — номер задачи обновления	Отменить задачу обновления
-c:current_update_id		Получить номер текущего обновления
-c:get_update_parameters		Получить глобальные настройки сервера
-c:get_update_schedule		Получить расписание обновлений
-c:get_update_source_parameters		Получить параметры источника обновлений
-c:set_update_schedule	**-by_time:** — время запуска загрузки обновлений; **-enabled:** — доступные значения: • yes — задача обновления будет включена; • no — задача обновления будет выключена	Настроить обновление по расписанию

Команда	Возможные аргументы	Действие
-c:set_update_ source_parameters	**-source:** — тип источника обновлений. Доступные значения: • https — загрузка обновлений с сервера компании "Код Безопасности" или с других локальных серверов обновления в компании (для режима каскадирования); • directory — загрузка обновлений из локальной папки; **-updates_host:** — адрес сервера обновлений; **-updates_port:** — порт сервера обновлений; **-eset_user_name:** — имя пользователя для лицензии ESET. Настройка данного параметра не требуется; **-download_block_size:** — размер блока в байтах, при скачивании с HTTP-ресурса. При большом размере блока (мегабайты) и медленном соединении возможно частое прерывание команды из-за сетевых тайм-аутов. При быстром соединении (минимально 100 Мбит/с) можно указать значение 1048576 байт (1Mb); **-download_timeout:** — тайм-аут скачивания в секундах; **-time_between_retries:** — время между попытками скачивания в секундах; **-download_retry_count:** — количество попыток скачивания; **-proxy_mode:** — режим работы прокси-сервера. Доступные значения: • custom_settings — ручная настройка прокси-сервера; • direct_connection — используется прямой доступ в Интернет; • system_proxy — использование настроек прокси-сервера, передаваемых по сети через DHCP/DNS. Не рекомендуется использовать данные настройки; **-proxy_address:** — адрес прокси-сервера (IP-адрес или имя сервера); **-proxy_port:** — порт прокси-сервера; **-proxy_authentication:** — тип авторизации на прокси-сервере. Доступные значения: • no — не требуется авторизация; • yes — требуется авторизация; **-proxy_user_name:** — имя пользователя для авторизации на прокси-сервере; **-proxy_password:** — пароль пользователя для авторизации на прокси-сервере; **-updates_source_directory:** — путь к папке локального сервера обновлений	Указать источник обновлений

Команда	Возможные аргументы	Действие
-c:set_update_ parameters	**-keep_packages:** — количество хранимых пакетов обновлений. Если обслуживаются клиенты, использующие локальное (быстрое) подключение, рекомендуемое число пакетов — 4, если обслуживаются удаленные клиенты, использующие медленное подключение, рекомендуемое число — 10; **-max_update_job_storage_time:** — количество дней, в течение которых будет храниться информация о выполненных задачах обновления в системе. Рекомендуемые значения — 20-40 дней	Изменить настройки хранения пакетов обновлений и утилит обновления

Загрузка обновлений с сервера обновлений

Пример 1

Настройка обновления антивирусных баз с локального сервера обновлений, расположенного в сети компании по адресу 192.168.221.1:

```
avus.exe -c:set_update_source_parameters -source:https -
updates_host:192.168.221.1
```

Пример 2

Настройка обновления антивирусных баз с сервера компании "Код Безопасности" через прокси-сервер с авторизацией:

```
avus.exe -c:set_update_source_parameters -source:https -
updates_host:updates.securitycode.ru -proxy_mode:custom_
settings -proxy_address:192.168.50.150 -proxy_port:8080 -
proxy_authentication:yes -proxy_user_name:domain\TestUser -
proxy_password:Password123
```

Примечание.

- Поддерживается только NTLM авторизация на прокси-сервере.
- На прокси-сервере рекомендуется предоставить анонимный доступ компьютерам, на которых располагаются серверы обновлений, используя проверку по MAC-адресу.

Пример 3

Настройка обновления антивирусных баз с сервера компании "Код Безопасности" без прокси-сервера:

```
avus.exe -c:set_update_source_parameters -source:https -
proxy_mode:direct_connection
```

Загрузка обновлений из папки

Пример 1

Настройка обновления антивирусных баз из локальной папки:

```
AVUS.exe -c:set_update_source_parameters -source:directory -
updates_source_directory:C:\new
```

Примечание. Необходимо убедиться, что учетная запись компьютера имеет доступ к содержимому указанной папки.

Настройка расписания обновлений

Время запуска загрузки обновлений задается в cron-формате согласно следующей схеме:

```
* * * * *
- - - - -
| | | | |
| | | | ----- День недели (0 - 7) (Воскресенье =0 или =7)
| | | ------- Месяц (1 - 12)
| | --------- День (1 - 31)
| ----------- Час (0 - 23)
------------- Минута (0 - 59)
```

Пример 1

Чтобы создать задание, предписывающее загружать доступные обновления ежедневно каждые четыре часа, выполните команду:

```
avus.exe -c:set_update_schedule -enabled:yes -by_time:"0 */4
* * *"
```

Пример 2

Для загрузки обновлений по субботам в 8 утра:

```
avus.exe -c:set_update_schedule -enabled:yes -by_time:"0 8 *
* 6"
```

Пример 3

Для настройки количества хранимых пакетов обновлений и времени хранения информации о выполненных обновлениях:

```
avus.exe -c:set_update_parameters -max_update_job_storage_
time:40 -keep_packages:4
```

Утилита обновления

В состав ПО Secret Net Studio входит утилита для автономного обновления антивирусных баз. При запуске утилиты осуществляется проверка текущей версии антивирусных баз для установленного антивируса. При необходимости выполняется установка актуальных обновлений, которые содержатся в утилите.

Утилиту обновления можно скачать на сайте компании "Код Безопасности" или на локальном сервере обновлений (см. раздел "Утилита обновления" в документе "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Примечание. В Secret Net Studio 8.2 входящий сетевой трафик на локальных серверах обновлений состоит из пакетов обновлений и утилит обновления (см. стр. 13).

Глава 3
Обновление ПО

Для обновления ПО серверов обновлений:

1. На компьютерах с установленным ПО серверов обновлений запустите установку компонента "Антивирус - сервер обновлений" новой версии (см. стр. 7). Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки. После подтверждения принятия условий лицензионного соглашения программа установки автоматически обновит предыдущую версию ПО.
2. Выполните процедуру обновления баз антивирусов на защищаемых компьютерах (см. раздел "Обновление антивирусных баз" в документе "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений").

Примечание. Обновление баз антивирусов Secret Net Studio версии 8.2 с серверов обновлений версий 8.0 или 8.1 не поддерживается.

Глава 4
Удаление сервера обновлений

Совет. Удаление также можно выполнить с помощью элемента "Программы и компоненты" из Панели управления ОС Windows.

Для удаления программного обеспечения:

1. Нажмите кнопку "Удалить" в диалоге "Изменение, восстановление или удаление установки".

   На экране появится диалог с сообщением о готовности к удалению.
2. Нажмите кнопку "Удалить".

   Начнется удаление установленных компонентов. После успешного завершения процесса удаления на экране появится диалог с сообщением об этом.
3. Нажмите кнопку "Готово".
4. Удалите каталог C:\ProgramData\Security Code\Secret Net Studio\Server\Antivirus Update Server (C:\ProgramData\Security Code\Secret Net Studio\Server\Antimalware Update Server).