КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Сервер обновлений. Установка и настройка

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

Оглавление

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для развертывания и настройки средства автоматического обновления антивирусных баз и баз решающих правил системы обнаружения вторжений 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" (https://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 https://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

Сервер обновлений предназначен для централизованного обновления баз следующих компонентов Secret Net Studio:

- Антивирус;
- Антивирус (технология ESET);
- Механизм обнаружения вторжений.

Обновление осуществляется с помощью следующих компонентов:

- глобальный сервер обновлений — сервер компании "Код Безопасности", который обеспечивает раздачу обновлений по адресу https://updates.securitycode.ru;
- локальный сервер обновлений — сервер обновлений, установленный в компании, который принимает обновления с глобального сервера обновлений;
- клиент сервера обновлений — компонент, обеспечивающий загрузку обновлений непосредственно на защищаемом компьютере. Клиент сервера обновлений входит в состав клиента Secret Net Studio (см. документ [**2**]).

Системные требования

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

- Windows 7 x86/x64 SP1;
- Windows 8.1 x86/x64 Rollup Update;
- Windows 10 x86/x64;
- Windows Server 2008 x64 R2 SP1;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2016.

Примечание. Не поддерживается работа сервера обновлений на компьютере с Windows Server Core.

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

На компьютере, предназначенном для сервера обновлений, должны быть установлены распространяемый компонент Microsoft Visual C++ Redistributable 2017 и платформа Microsoft .NET Framework 4.5.

Для работы сервера обновлений на компьютере должен быть открыт исходящий порт 43444.

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

Примечание. В Secret Net Studio версии 8.4 входящий сетевой трафик на локальных серверах обновлений состоит из пакетов обновлений.

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 обновление антивирусных баз с сервера компании "Код Безопасности" (см. документ [**7**]).

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 обновление антивирусных баз с локального сервера (см. документ [**7**]).

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 (см. стр.**19**).

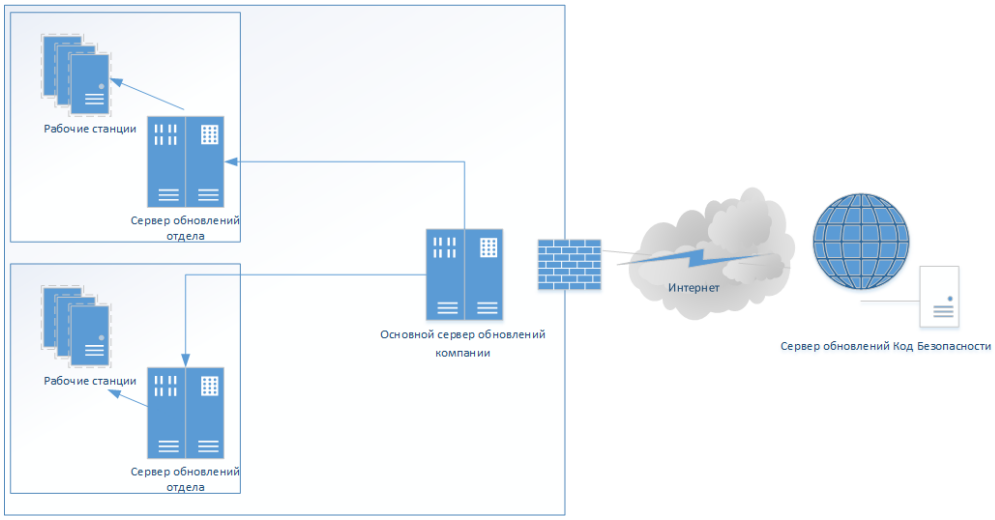
В программе управления Secret Net Studio для каждого защищаемого компьютера необходимо настроить обновление антивирусных баз с локального сервера и указать адрес сервера в закрытой сети, данные на который переносятся вручную (см. документ [**7**]).

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 (см. стр.**19**).

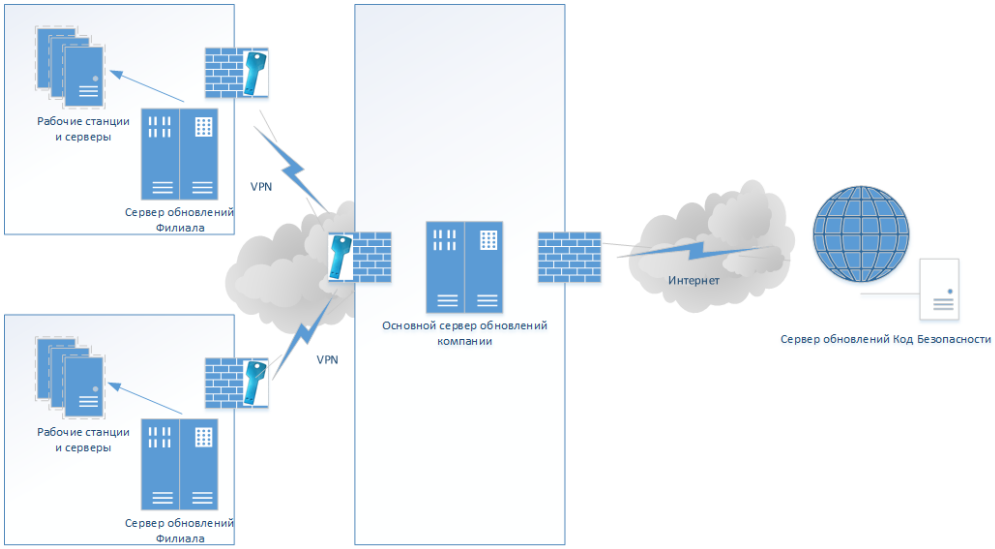
Пример 1. В компании используется несколько подсетей.

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

План установки и настройки сервера обновлений

1. Выполните предварительную настройку компьютера, предназначенного для сервера обновлений (см. стр.**8**).
2. Выполните установку ПО Сервера обновлений Secret Net Studio (см. стр.**8**).
3. Настройте загрузку обновлений с сервера компании "Код Безопасности", с локального сервера обновлений или из локальной/сетевой директории (см. стр.**12**).
4. При необходимости настройте расписание обновлений (см. стр.**14**).
5. Укажите значения параметров загрузки обновлений (см. стр.**14**).
6. Выберите компоненты Secret Net Studio, обновление баз которых необходимо выполнять (см. стр.**15**).
7. Запустите загрузку обновлений, нажав кнопку "Загрузить обновления" на панели инструментов, или дождитесь обновления по расписанию.

Примечание. Чтобы прервать процесс загрузки обновлений, нажмите кнопку "Остановить загрузку обновлений".

Предварительная настройка компьютера

На компьютер, предназначенный для сервера обновлений Secret Net Studio, необходимо предварительно установить дополнительное ПО.

Для установки дополнительного ПО:

1. Установите распространяемый компонент Microsoft Visual C++ Redistributable 2017. Для этого запустите с установочного диска из каталога \Tools\Microsoft\Prerequisites файл vcredist_ x64 или vcredist_ x86 (в зависимости от версии установленной на компьютере ОС Windows) и следуйте указаниям мастера установки.
2. Установите сервер IIS версии 7 или выше.
3. Установите Microsoft .NET Framework 4.5.
4. В настройках брандмауэра Windows Server откройте порт 43444 для исходящих подключений.

Установка сервера обновлений

Для установки сервера обновлений:

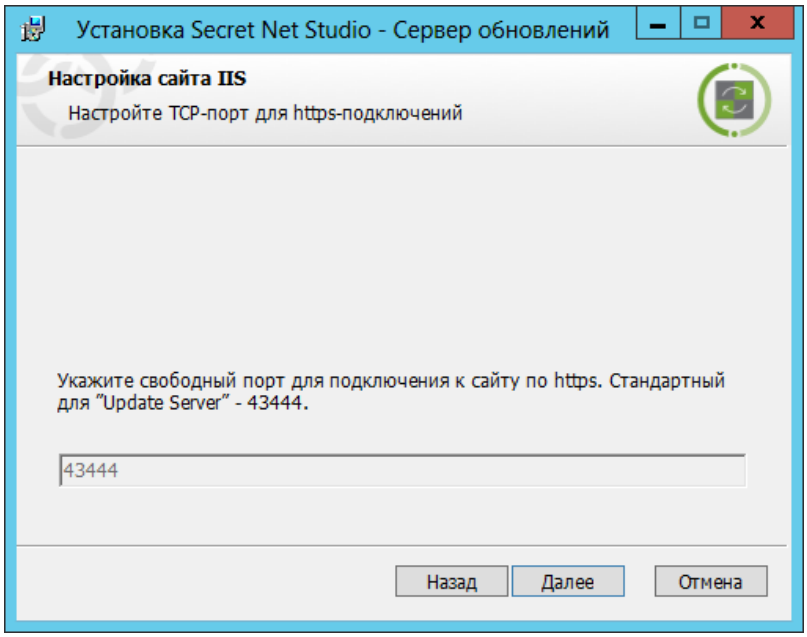
1. Войдите в систему с правами администратора компьютера.
2. Запустите на исполнение файл UpdateServer.msi от имени администратора.

   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".

На экране появится окно настройки порта для HTTPS-подключений.



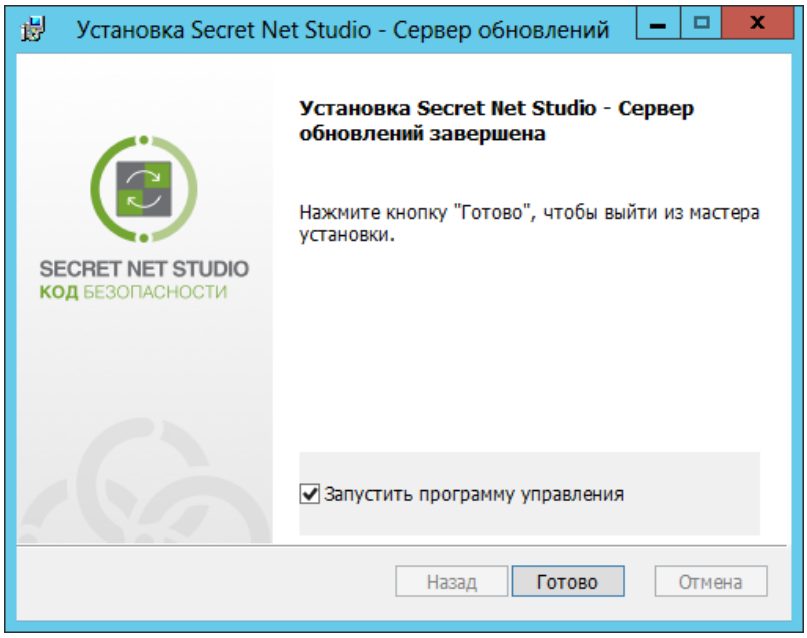
По умолчанию используется порт 43444.

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

5. 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.



6. Отметьте пункт "Запустить программу управления", чтобы программа управления сервером обновлений открылась автоматически по завершении работы мастера установки. Нажмите кнопку "Готово".

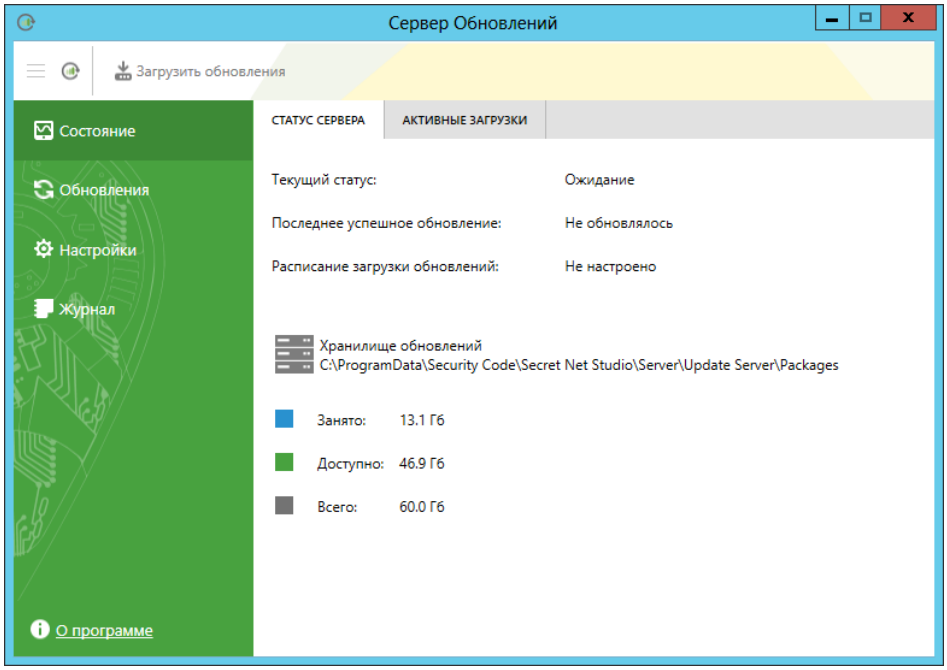
Программа управления сервером обновлений

Установленный сервер обновлений располагается в каталоге C:\Program Files\Secret Net Studio\Server\Update Server.

Чтобы запустить программу управления сервером обновлений, выберите в меню "Пуск" команду "Приложения | Код Безопасности | Secret Net Studio | Сервер обновлений".

Примечание. На компьютере с ОС Windows 10 в меню "Пуск" не отображается папка "Secret Net Studio".

Откроется окно программы "Сервер Обновлений".



Главное меню программы управления содержит разделы:

- Состояние (см. стр.**10**);
- Обновления (см. стр.**11**);
- Настройки (см. стр.**12**);
- Журнал (см. стр.**16**).

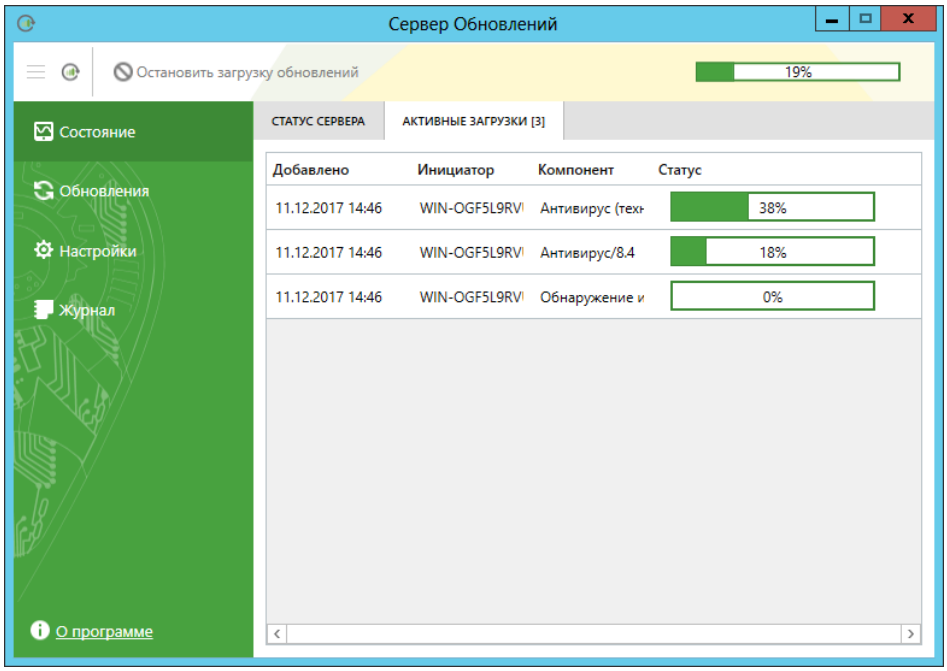
Просмотр информации о состоянии сервера

На вкладке "Статус сервера" в разделе "Состояние" находится информация о текущем состоянии сервера обновлений и о доступном пространстве в каталоге, на котором расположено хранилище пакетов обновлений.

На странице отображаются следующие данные:

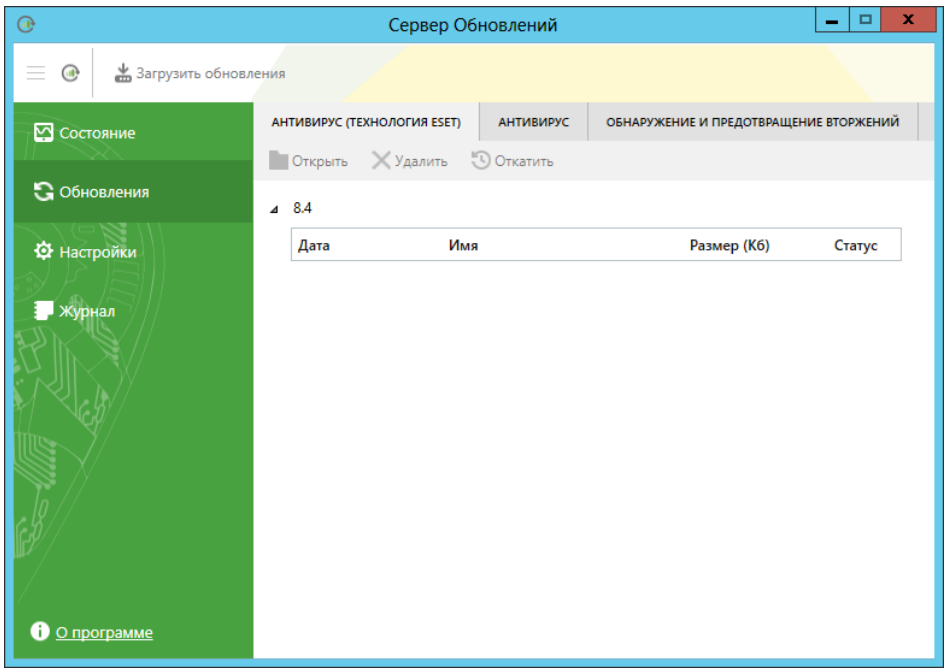
- текущий статус загрузки обновлений;
- дата и время последнего успешного обновления;
- дата и время обновления по расписанию;
- путь к хранилищу обновлений;
- размер использованного дискового пространства;
- размер свободного дискового пространства, доступного для данной папки с учетом квоты;
- общий размер хранилища.

Чтобы просмотреть информацию о ходе выполнения загрузки обновлений, перейдите на вкладку "Активные загрузки".



Просмотр информации об обновлениях

На вкладках "Антивирус", "Антивирус (Технология ESET)" и "Обнаружение и предотвращение вторжений" в разделе "Обновления" содержатся списки всех пакетов обновлений антивирусных баз и баз решающих правил, хранящихся на сервере.



Для каждого обновления отображаются дата выпуска пакета, имя и размер, а также статус:

- текущее обновление;
- резервное обновление;
- недоступно (например, если файл обновления был удален в обход средств управления сервером обновлений).

Для пакетов обновлений доступны следующие действия.

Элемент	Назначение
Открыть	Выберите обновление и нажмите кнопку "Открыть", чтобы открыть директорию с файлом обновления
Удалить	Выберите пакет обновлений, нажмите кнопку "Удалить" и подтвердите действие в появившемся окне. Будут удалены все файлы, относящиеся к данному пакету обновлений. Возможно удаление только резервных и недоступных обновлений
Откатить	Нажмите, чтобы выполнить восстановление выбранной версии баз. Команда доступна только для резервных обновлений

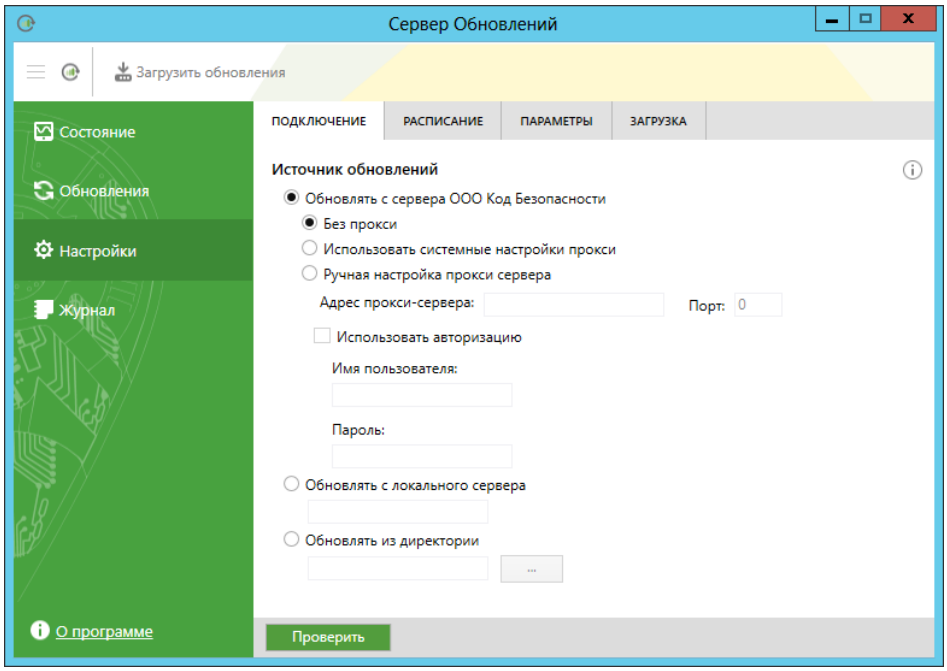
Настройка сервера обновлений

Подключение к источнику обновлений

Для работы сервера обновлений необходимо настроить подключение к источнику обновлений.

Для выбора источника обновлений:

1. В разделе "Настройки" перейдите на вкладку "Подключение".



2. Выберите источник обновлений.
   - Обновлять с сервера ООО Код Безопасности — выберите данный пункт, чтобы загружать обновления баз напрямую с глобального сервера обновлений. При необходимости настройте параметры прокси-сервера.

Параметр	Описание
Без прокси	Выберите данный пункт, если соединение с сервером обновлений происходит напрямую (без прокси-сервера)
Использовать системные настройки прокси	Используется автоматическое определение прокси-сервера
Ручная настройка прокси-сервера	Выберите данный пункт, чтобы настроить прокси-сервер вручную. Укажите адрес прокси-сервера и порт. Если на прокси-сервере используется авторизация, укажите имя пользователя и пароль

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.

   - Обновлять с локального сервера — выберите, если в локальной сети установлен сервер обновлений Secret Net Studio, и укажите адрес сервера;
   - Обновлять из директории — выберите данный пункт, если обновления находятся в локальной или сетевой папке. Укажите путь к директории, используя окно "Обзор папок".

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

Примечание. Обновление из сетевой папки возможно только в рамках домена. Для корректной работы необходимо предоставить доступ на чтение к сетевой папке всем авторизованным пользователям или учетным записям компьютеров, ПО которых будет обновлено таким способом.

3. Чтобы проверить доступность загрузки обновлений с выбранного источника, нажмите кнопку "Проверить".

   На экране появится результат проверки.

4. Нажмите кнопку "Сохранить", чтобы сохранить настройки конфигурации сервера обновлений.

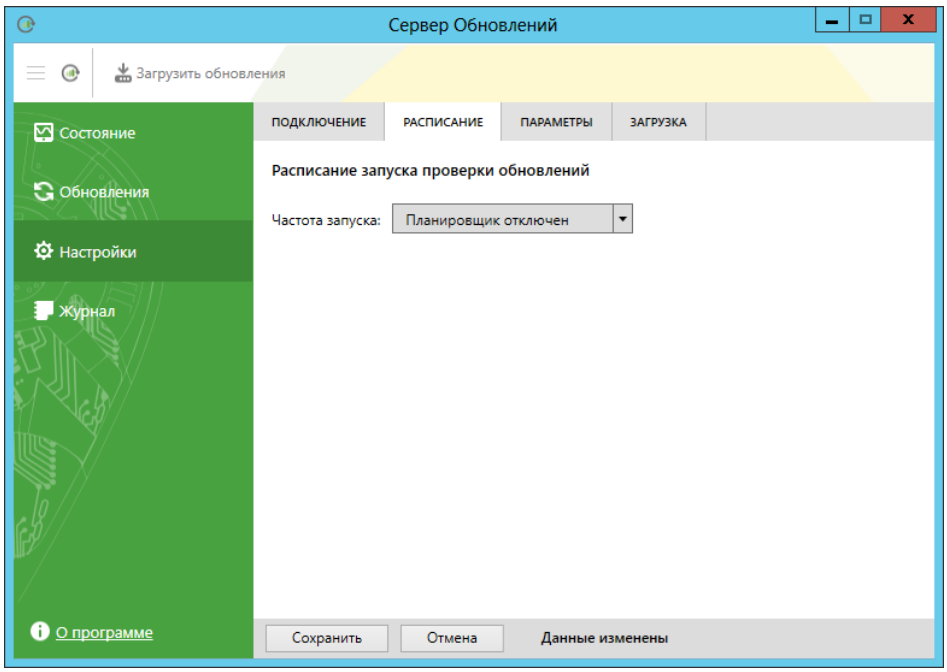
Примечание. Используйте кнопку "Отмена", чтобы сбросить изменения конфигурации сервера.

Настройка расписания обновлений

Время запуска загрузки обновлений может быть настроено.

Для настройки расписания:

1. В разделе "Настройки" перейдите на вкладку "Расписание".



2. Выберите частоту запуска проверки обновлений из раскрывающегося списка и укажите параметры даты и времени обновления.

Примечание. Рекомендуется выполнять обновление баз каждые 3-4 часа.

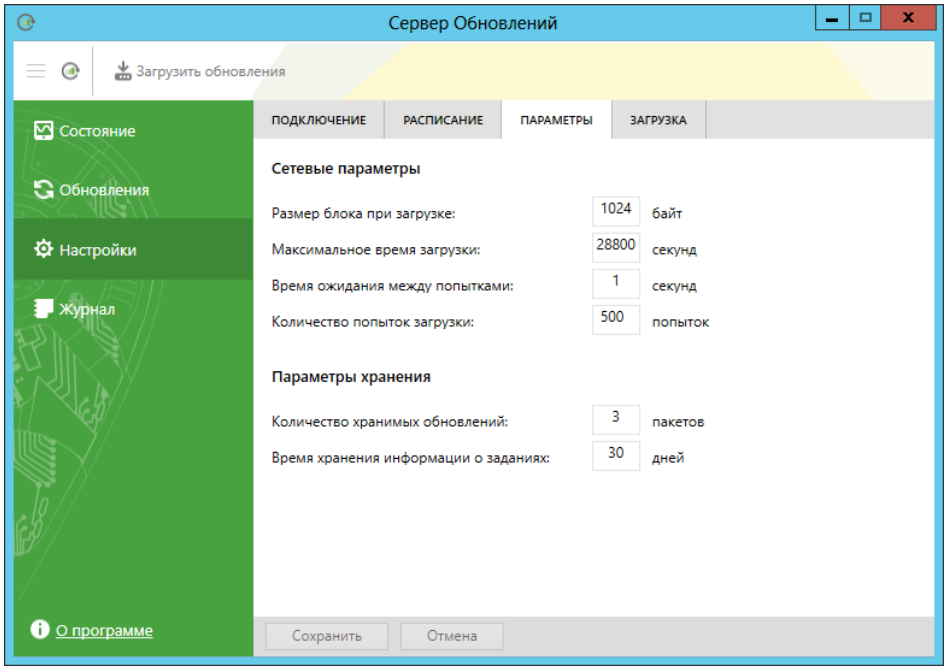
3. Нажмите кнопку "Сохранить", чтобы изменения вступили в силу.

Примечание. Используйте кнопку "Отмена", чтобы сбросить изменения в расписании обновления.

Настройка параметров загрузки обновлений

Для настройки параметров загрузки:

1. В разделе "Настройки" перейдите на вкладку "Параметры".



2. Введите значения сетевых параметров.

Элемент	Назначение
Размер блока при загрузке	Размер блока данных при загрузке через HTTPS. Минимальное значение — 1024, максимальное — 10485760
Максимальное время загрузки	Время ожидания загрузки обновлений. Минимальное значение — 100, максимальное — 36000
Время ожидания между попытками	Время ожидания между попытками загрузки обновлений. Минимальное значение — 1, максимальное — 100
Количество попыток загрузки	Количество попыток загрузки обновлений. Минимальное значение — 1, максимальное — 500

3. Укажите значения параметров хранения обновлений.

Элемент	Назначение
Количество хранимых обновлений	Количество хранимых пакетов обновлений. Минимальное значение — 1, максимальное — 100
Время хранения информации о заданиях	Время хранения информации о выполненных заданиях обновления. Минимальное значение — 1, максимальное — 365

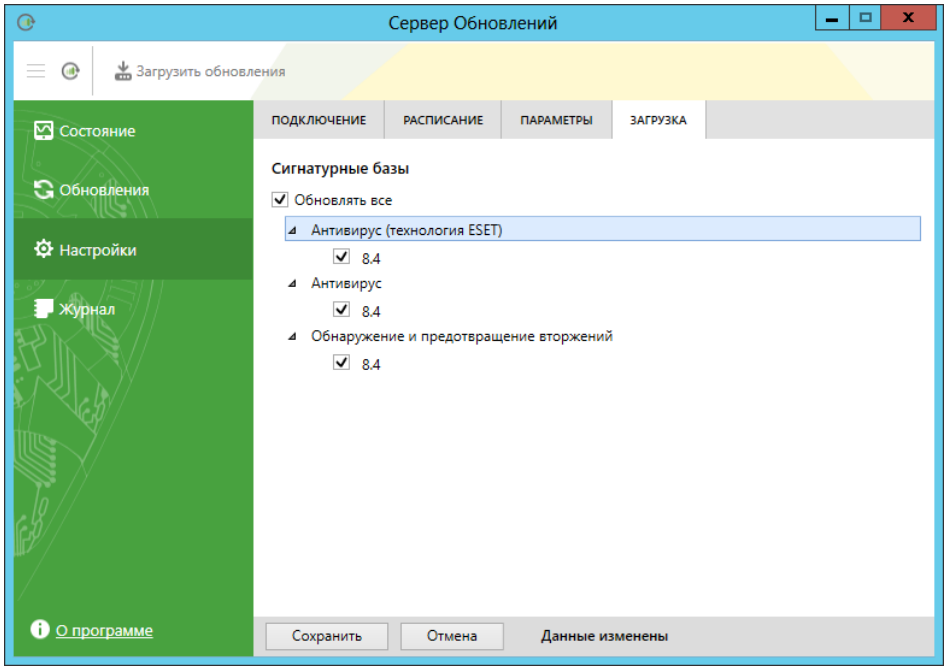
4. Нажмите кнопку "Сохранить", чтобы изменения вступили в силу.

Примечание. Используйте кнопку "Отмена", чтобы сбросить изменения параметров загрузки обновлений.

Выбор компонентов для обновления

Для выбора компонентов:

1. В разделе "Настройки" перейдите на вкладку "Загрузка".



2. Выберите компоненты Secret Net Studio, базы которых должны быть обновлены, и нажмите кнопку "Сохранить", чтобы изменения вступили в силу.
3. После выбора компонентов на экране появится сообщение с предложением загрузить обновления для добавленных компонентов или удалить все обновления для компонентов, которые не были отмечены. Нажмите кнопку "Загрузить"/"Удалить" соответственно.

Примечание. Используйте кнопку "Отмена", чтобы сбросить изменения.

Просмотр журнала операций

В журнале отображается информация об операциях, выполненных на сервере обновлений в текущей сессии. Чтобы открыть журнал в главном меню программы управления, выберите пункт "Журнал".

При закрытии программы управления журнал операций автоматически очищается.

Глава 3
Обновление ПО

Для обновления ПО серверов обновлений:

1. На компьютерах с установленным ПО серверов обновлений запустите установку компонента "Сервер обновлений" новой версии (см. стр. **8**). 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 и баз решающих правил на защищаемых компьютерах (см. раздел "Обновление" в документе [**7**]).

Глава 4
Удаление сервера обновлений

Программа установки сервера обновлений Secret Net Studio позволяет удалить установленное ПО с компьютера.

Перед тем как приступить к выполнению этих действий, завершите работу программы управления сервером обновлений.

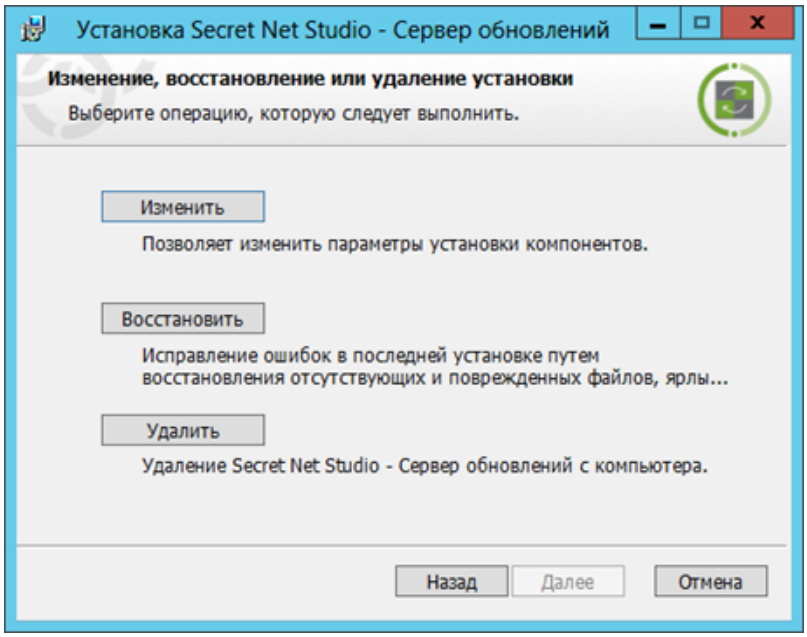
Совет. Удаление также можно выполнить с помощью элемента "Программы и компоненты" из Панели управления ОС Windows.

Для удаления программного обеспечения:

1. Запустите программу установки.

   Программа выполнит подготовительные действия и выведет на экран диалог приветствия.
2. Нажмите кнопку "Далее".

   На экране появится диалог "Изменение, восстановление или удаление установки".



3. Нажмите кнопку "Удалить".

   Начнется удаление установленных компонентов. После успешного завершения процесса удаления на экране появится диалог с сообщением об этом.
4. Нажмите кнопку "Готово".
5. Удалите каталог C:\Program Files\Secret Net Studio\Server\Update Server.

Приложение

Загрузка обновлений с сетевого ресурса

Для загрузки обновлений с сетевого ресурса:

1. Установите ПО сервера обновлений на компьютере с доступом к интернету.
2. Настройте обновление с сервера компании "Код Безопасности" (см. стр.**12**) и убедитесь в том, что загрузка обновлений выполняется успешно.
3. Создайте сетевой ресурс и предоставьте к нему доступ авторизованным пользователям. Доступ к пакетам обновлений будет происходить от имени компьютеров, на которых будут работать антивирусы или каскадные серверы обновлений.
4. Настройте синхронизацию содержимого папки C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages с нужным сетевым ресурсом.

Примечание. Настроить синхронизацию данных можно с помощью любой утилиты для репликации каталогов, например, Robocopy (входит в состав Windows Vista и выше).

Перенос обновлений вручную

При необходимости переноса обновлений вручную скопируйте каталог C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages или синхронизируемый с ним каталог (см. выше) на съемный носитель информации и перенесите на сервер в закрытой сети.

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.

Внимание! Утилита содержит в себе обновление только одного из антивирусов.

При установке обновлений выполняется проверка совместимости содержимого загруженного архива с версией продукта, установленного на защищаемом компьютере. Также выполняется верификация и проверка целостности архива.

Утилиту можно скачать на сайте компании "Код Безопасности" или на локальном сервере обновлений.

Для загрузки и запуска утилиты:

1. Перейдите по ссылке https://updates.securitycode.ru:43444.
2. Чтобы скачать утилиту, нажмите на ссылку:
   - "Пакет обновлений антивирусной базы антималваре";
   - "Пакет обновлений антивирусной базы".

   Примечание. В имени файла указана версия антивирусной базы, которая содержится в утилите.
3. На защищаемом компьютере запустите на исполнение загруженный файл утилиты. На экране появится сообщение о результате обновления антивирусных баз.

   Примечание. При отсутствии необходимого свободного места на диске обновления не будут установлены.

Если во время применения обновления произошел сбой, возврат к предыдущей версии баз произойдет автоматически. В остальных случаях возврат к предыдущим версиям антивирусных баз возможен только средствами утилиты

av_cli.exe (см. документ [**7**]) или программы управления сервером обновлений (см. стр.**10**).

Устранение неисправностей

При возникновении проблем в работе сервера обновлений Secret Net Studio следует просмотреть события аудита в журнале клиента Secret Net Studio (если он установлен на компьютере) или в журнале сервера обновлений.

Документация

1. Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
2. Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
3. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.001 91 3
4. Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
5. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
6. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
7. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
8. Средство защиты информации Secret Net Studio. Руководство администратора. Сервер обновлений. Установка и настройка	
9. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92