Оповещение службы поддержки

Уведомление о необходимости обновления программного обеспечения

Обновление программного обеспечения касается информационных систем «АСДКиУ», «Comfort Contour» и «Comfort Contour Pro» (далее системы) построенных с использованием контроллеров «БКД-ПК-RF» и «ECA Connect» (далее контроллеры) и использующих для передачи данных встроенное в них программное обеспечение «OpenVPN».

1. Причина обновления

Встроенное программное обеспечение контроллеров предусматривает возможность передачи данных с использованием технологии виртуальной частной сети (VPN). Для этого использовано программное обеспечение «OpenVPN» - свободная реализация технологии VPN с открытым исходным кодом.
Для аутентификации контроллеров на сервере VPN используется сертификаты X.509. Срок действия серверного и клиентских сертификатов ограничен максимальным значением 3650 суток. Срок действия входящего в состав дистрибутивов систем серверного сертификата и подписанных им клиентских сертификатов контроллеров заканчивается 25-04-2019 в 13:15:39 GMT. По истечении этой даты контроллеры не смогут подключиться к серверу VPN.

2. В каких случаях обновление не требуется

Обновление необходимо для систем диспетчеризации использующих передачу данных с использованием «OpenVPN». Если в Вашем случае использование встроенного клиента «OpenVPN» отключено в настройках контроллеров и используется технология виртуальной частной сети предоставляемая оператором сотовой связи или проводным интернет-провайдером или используется прямое подключение к серверу в рамках локальной сети предприятия, то обновление программного обеспечения или выполнение каких-либо других действий не требуется.

3. Способы решения

Существует два способа решения описанной проблемы:

1. Первый способ заключается в необходимости заблаговременного (до момента окончания срока службы действующего сертификата) перевыпуска серверного и клиентских ключей и сертификатов, записи новых ключей и сертификатов на сервер и во все контроллеры. Данный способ описан в официальной документации «OpenVPN» (https://openvpn.net/vpn-server-resources/#documentation) и других источниках в сети интернет (https://sysadmins.ru/topic419705.html, https://forums.openvpn.net/viewtopic.php?t=18671).

Недостатками данного способа на наш взгляд являются высокая трудоемкость, необходимость достаточно высокой квалификации сотрудников, перерывы в функционировании информационной системы на время когда на части контроллеров сертификаты уже обновлены, а на другой части еще нет.

2. Второй способ заключается в установке модифицированной версии программы «OpenVPN» игнорирующей факт истечения срока действия серверного и клиентских сертификатов. В рамках поддержки работы перечисленных информационных систем нами выполнены работы по подготовки модифицированных версий программы «OpenVPN» для контроллеров и серверов работающих под управлением операционных систем «Windows» (32

и 64 бита) и «Linux Ubuntu Server» (32 и 64 бита). Второй способ значительно более прост в использовании и при заблаговременном применении позволит избежать перерывов в функционировании информационных систем.

Выбор способа обновления должен быть выполнен специалистами IT-служб организации, эксплуатирующей указанные информационные системы.

При выборе первого способа все работы по обновлению сертификатов и ключей должны быть выполнены силами IT-служб эксплуатирующей организации.

Как разработчик указанных информационных систем мы рекомендуем использование второго способа. Дальнейшая часть данного документа посвящена реализации второго способа решения по обновлению.

4. Технические подробности

Программа «OpenVPN» выпускается под свободной лицензией «GPL v.2» допускающей модификацию исходного кода при условии его открытой публикации. Суть модификации программы «OpenVPN» заключается в использовании программного изменения (патча) игнорирующего возникновение ошибки «X509_V_ERR_CERT_HAS_EXPIRED» при выполнении проверки сертификата. Остальные проверки сертификата сохраняются без изменения.

Для выпуска модифицированной версии сервера «OpenVPN» (версии для Windows 32/64 и Linux i686/x86_64) использованы версии 2.4.6 и 2.3.13 программы. Для выпуска модифицированной версии клиента «OpenVPN» (версии для контроллера Linux ARM 32) использована версия 2.2.1 программы.

Исходный текст изменения (патча) для указанных версий «OpenVPN» доступен по ссылке в интернете: ftp://www.mnppsaturn.ru/public/soft/ovpn_path/paths/.

Для проверки отсутствия других изменений и целостности при скачивании исполнимые модули и библиотеки «OpenVPN» подписаны цифровой подписью (имя: «MNPP SATURN, ООО», с/н: «00eb579592f7f2651d3deff7d09ee14945»).

5. Выполнение обновления

Для выполнения обновления необходимо обновить программное обеспечение «OpenVPN» на сервере системы и на всех контроллерах «БКД-ПК-RF» и «ECA Connect». Порядок обновления не важен: до истечения срока действия сертификатов обновленные клиенты «OpenVPN» могут подключаться к не обновленному серверу «OpenVPN» и наоборот, не обновленные клиенты могут подключаться к обновленному серверу. После истечения срока действия сертификатов возможно подключение только обновленных клиентов к обновленному серверу «OpenVPN».

5.1 Обновление ПО контроллеров

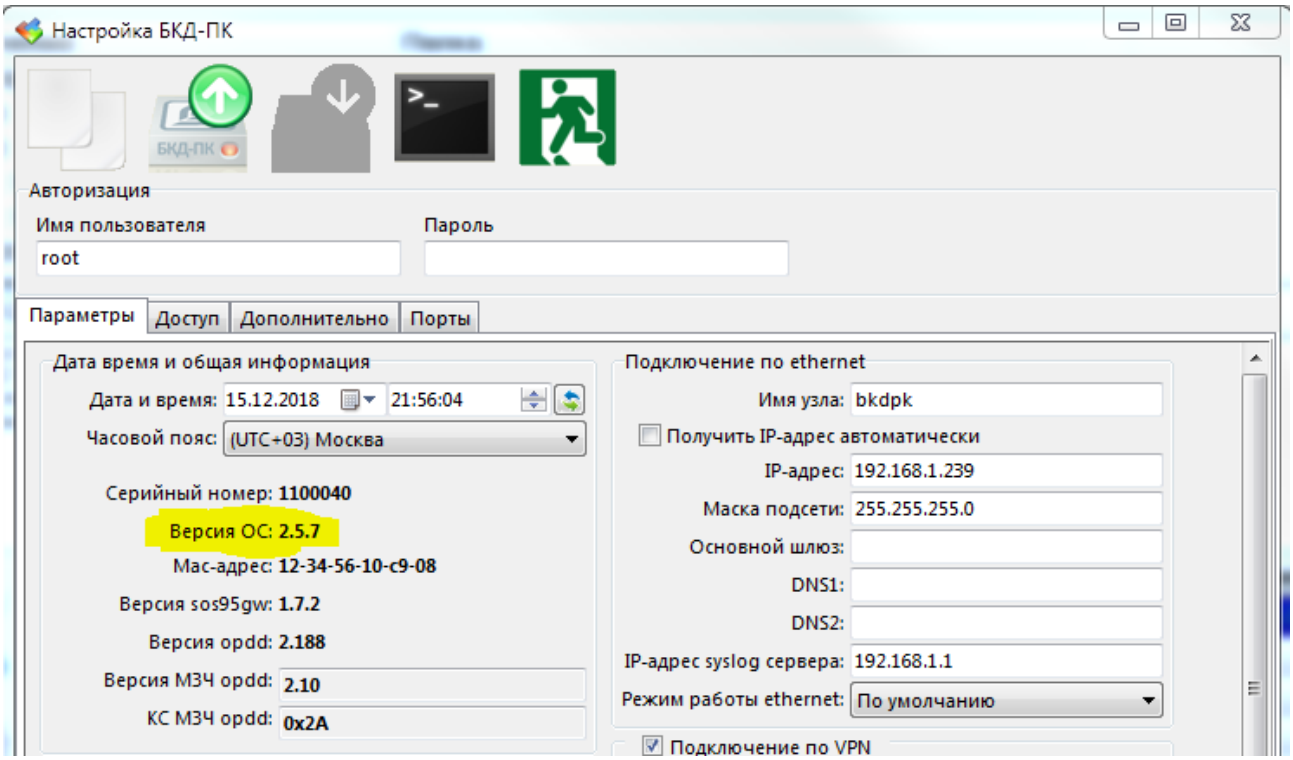
Обновление ПО контроллеров может быть выполнено в автоматическом или ручном режимах.

5.1.1 Автоматический режим обновления ПО контроллеров

Автоматический режим обновления доступен для контроллеров имеющих доступ к сети интернет через сеть оператора сотовой связи или проводного провайдера и выполняется при помощи встроенной в контроллеры службы автоматического обновления. Задание на автоматическое обновление всех доступных в сети интернет контроллеров дано в конце

декабря 2018 года и до середины января 2019 ПО всех доступных контроллеров должно быть обновлено.

Убедиться в том, что ПО контроллера уже обновлено можно при помощи программы настройки контроллеров «RASOS». У контроллеров с обновленным клиентом «OpenVPN» версия ОС должна быть 2.5.7 или более новой (см. рисунок ниже). Руководство по работе с программой «RASOS» входит в состав документации на информационную систему.



Служба автоматического обновления с целью проверки наличия обновлений запускается контроллером сразу после включения и далее периодически, один раз в сутки. Размер скачиваемого файла обновления с модифицированным клиентом «OpenVPN» составляет ~800 кБ. После получения обновления служба сама выполняет все необходимые действия по установке и запуску обновленного программного обеспечения.

Служба автоматического обновления не использует в своей работе «OpenVPN», поэтому автоматическое обновление возможно в том числе и после прекращения срока действия сертификата. Единственное необходимое условие для работы службы — наличие доступа через сеть интернет к серверу обновлений по протоколу HTTP. Контроллеры, которые были выключены (находились на складе, не использовались и т.п.) получат обновление сразу после первого включения и получения доступа в сеть интернет.

5.1.2 Ручной режим обновления ПО контроллеров

Ручной режим обновления необходимо использовать для контроллеров, которые не имеют доступа в сеть интернет. Это может быть в случаях, когда контроллеры работают в частной изолированной сети передачи данных организованной оператором сотовой связи или проводным провайдером, но тем не менее, при этом используется «OpenVPN». Кроме того, ручной режим может быть использован для обновления контроллеров у которых качество связи с сервером обновления не позволяет загрузить файл обновления в автоматическом режиме.

Для обновления вам необходимо загрузить файл обновления по ссылке:

ftp://www.mnppsaturn.ru/public/soft/ovpn_path/linux_arm_update/ovpn-85bba833ba5b2fc88fbb6e67aea31207.tar.gz.

Указанный файл необходимо записать по протоколу FTP в папку «/disk/update» в контроллеры.

ВАЖНО: нельзя переименовывать скачанный файл обновления, имя файла должно оставаться неизменным: «`ovpn-85bba833ba5b2fc88fbb6e67aea31207.tar.gz`».

После записи файла обновления в контроллер необходимо дать команду «reboot» через протокол «telnet» или выключить и затем включить питание контроллера.

Проверка правильности выполнения обновления может быть выполнена программой «RASOS» (см. выше).

5.2 Обновление ПО сервера и клиента ОС «Windows»

Обновление серверного и клиентского ПО «OpenVPN» для операционной системы «Windows» выполняется в ручном режиме в изложенной ниже последовательности.

5.2.1 Определение расположения файлов «OpenVPN»

Определите расположение исполнимых файлов «OpenVPN» в файловой системе. Обычно исполнимые файлы «OpenVPN» расположены в следующих папках:

Для 32-х разрядной версии «Windows»:

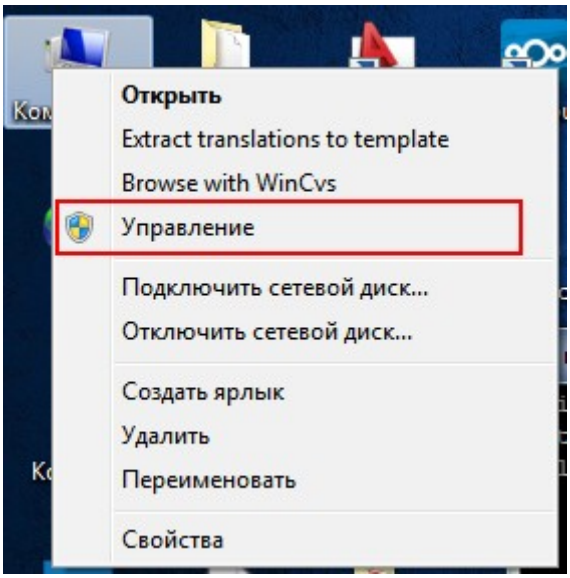
"C:\Program Files\OpenVPN\bin".

Для 64-х разрядной версии «Windows»:

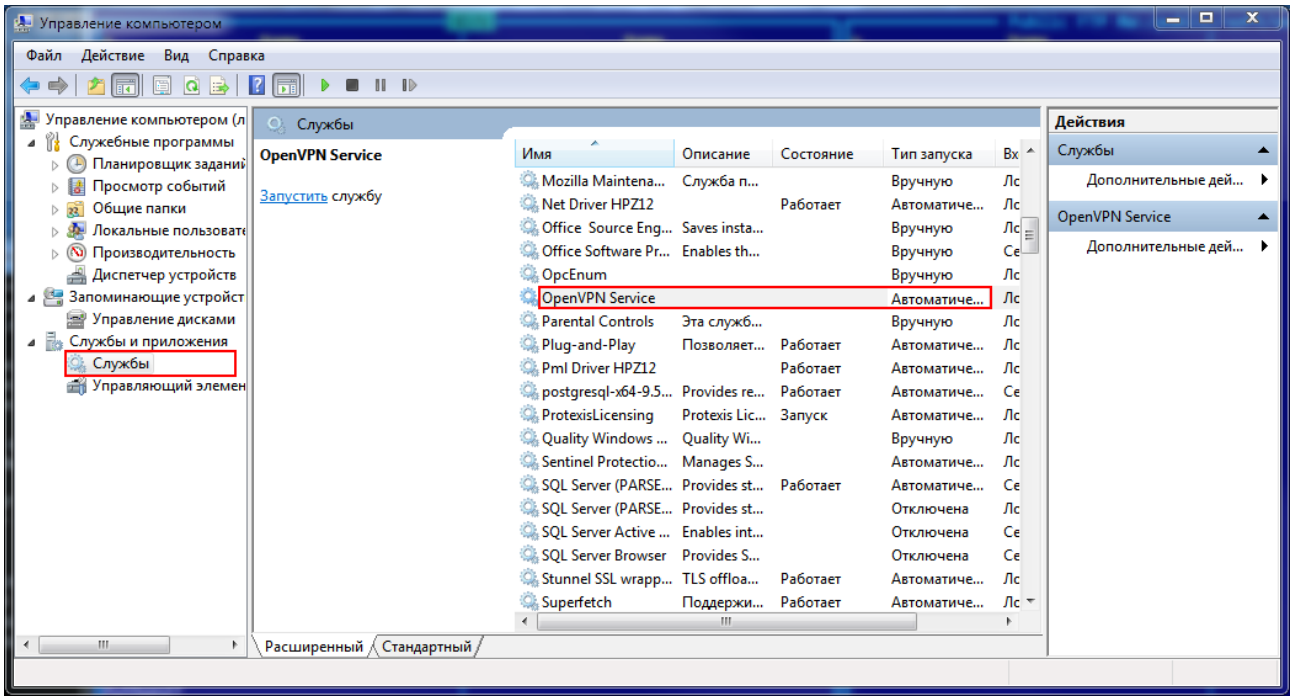
"C:\Program Files\OpenVPN\bin" (64-х разрядная версия) или
"C:\Program Files (x86)\OpenVPN\bin" (32-х разрядная версия).

Для уточнения места расположения и версии исполнимых файлов «OpenVPN» выполните следующие действия:

- На рабочем столе в контекстном меню иконки «Компьютер» выберите пункт «Управление».

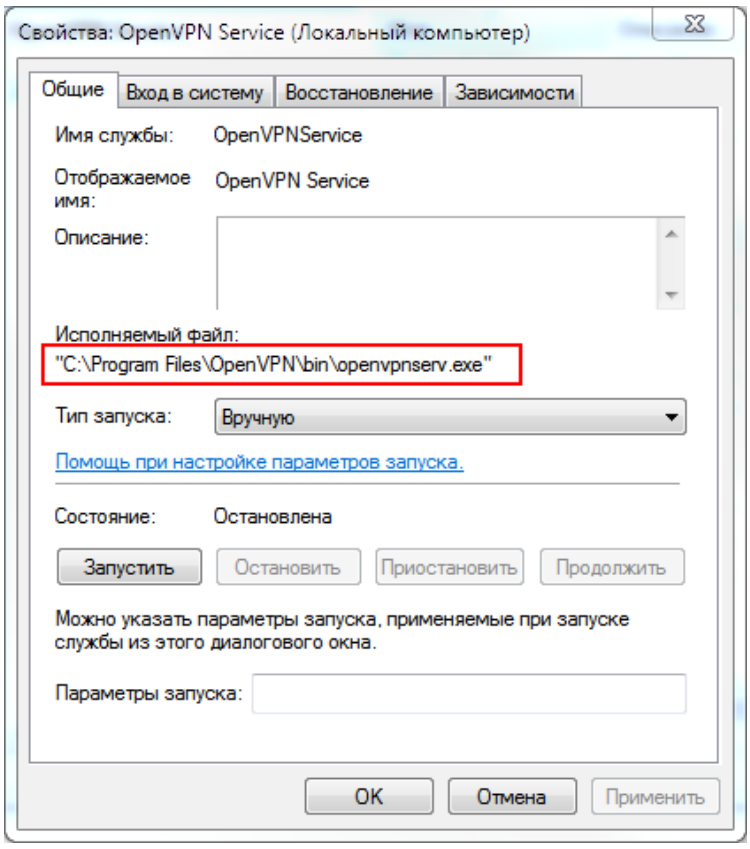


- В левой части окна «Управление компьютером» выберите пункт «Службы и приложения / Службы», в списке служб в правой части окна найдите и выберите службу «OpenVPN Service».



Если ваш компьютер выполняет функции сервера «OpenVPN», то в поле «Тип запуска» будет значение «Автоматически», если компьютер используется как клиент сервера «OpenVPN», то в поле будет значение «Вручную».

- Выполните двойной клик мышью по строке службы «OpenVPN Service».

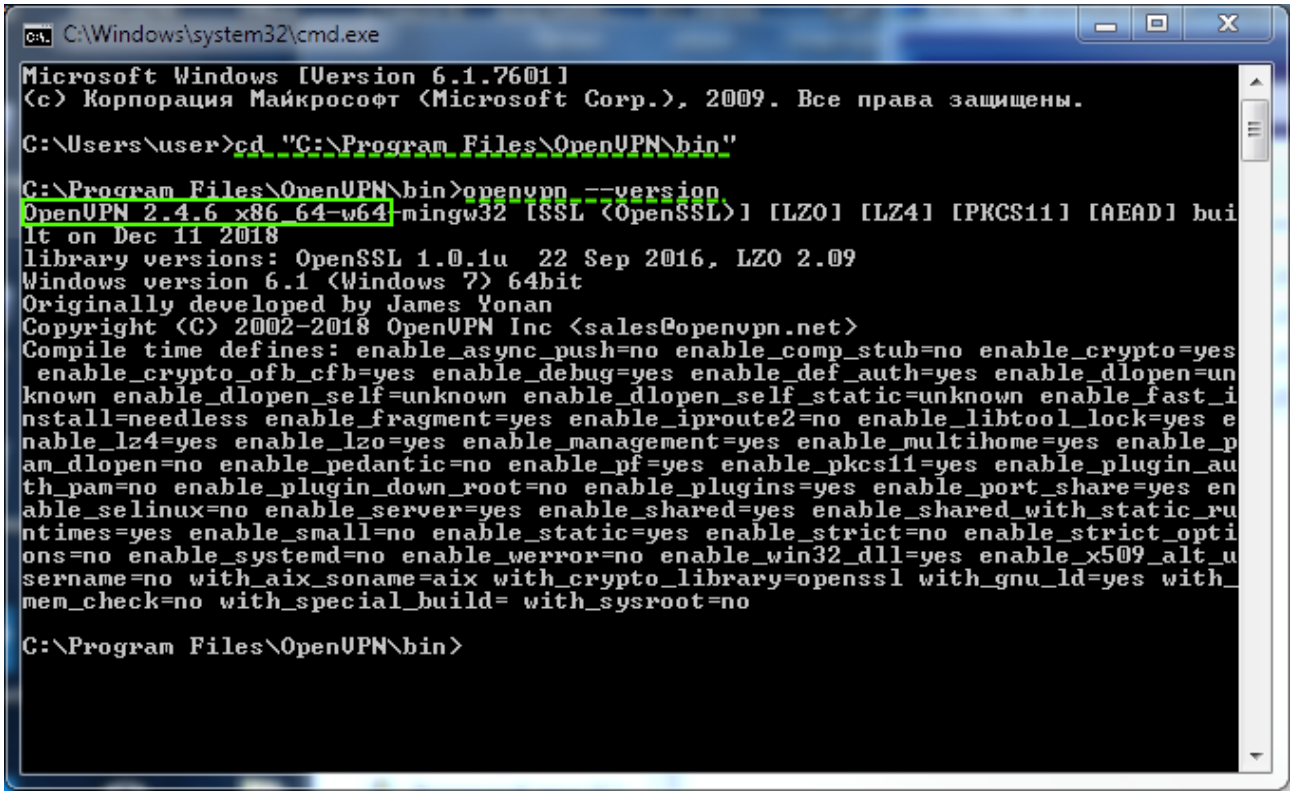


В поле «Исполняемый файл» будет указан путь папке, в которой расположены исполнимые файлы «OpenVPN».

5.2.2 Определение установленной версии «OpenVPN»

Откройте окно командной строки «Windows» (в строке поиска наберите «cmd» и нажмите клавишу «Ввод»).

Перейдите при помощи команды «cd» в папку в которой установлены исполнимые модули «OpenVPN», наберите команду «openvpn --version».



В результате выполнения команды будет отображена информация о версии «OpenVPN» (2.4.6 на примере выше) и его разрядности:

«i686-w64» - версия 32 бита;
«x86_64-w64» - версия 64 бита (как на примере выше).

5.2.3 Скачивание обновленной версии

Обновленные версии «OpenVPN» можно скачать по ссылке:
ftp://www.mnppsaturn.ru/public/soft/ovpn_path/bin/

По указанной ссылке находится четыре варианта для скачивания:

Название	Операционная система	Версия	Разрядность
2.3.13-win32	Windows	2.3.13	32
2.4.6-win32	Windows	2.4.6	32
2.4.6-win64	Windows	2.4.6	64
2.4.6-linux-i686	Linux	2.4.6	64

Версия «OpenVPN» 2.4.0 и более новые поддерживает работу только в «Windows Vista» и более новых. Версия TAP-драйвера 9.9 и более новые не совместимы с «Windows XP».

Скачайте архив с необходимой вам версией «OpenVPN» выбрав ее в соответствии с

следующими правилами:

- Если у вас установлена 32-х битная версия «OpenVPN», то необходимо скачать 32-х битную версию.

- Если у вас установлена 64-х битная версия «OpenVPN», то необходимо скачать 64-х битную версию.

- Если у вас установлена версия 2.3.x или более ранняя, то необходимо скачать версию 2.3.13.

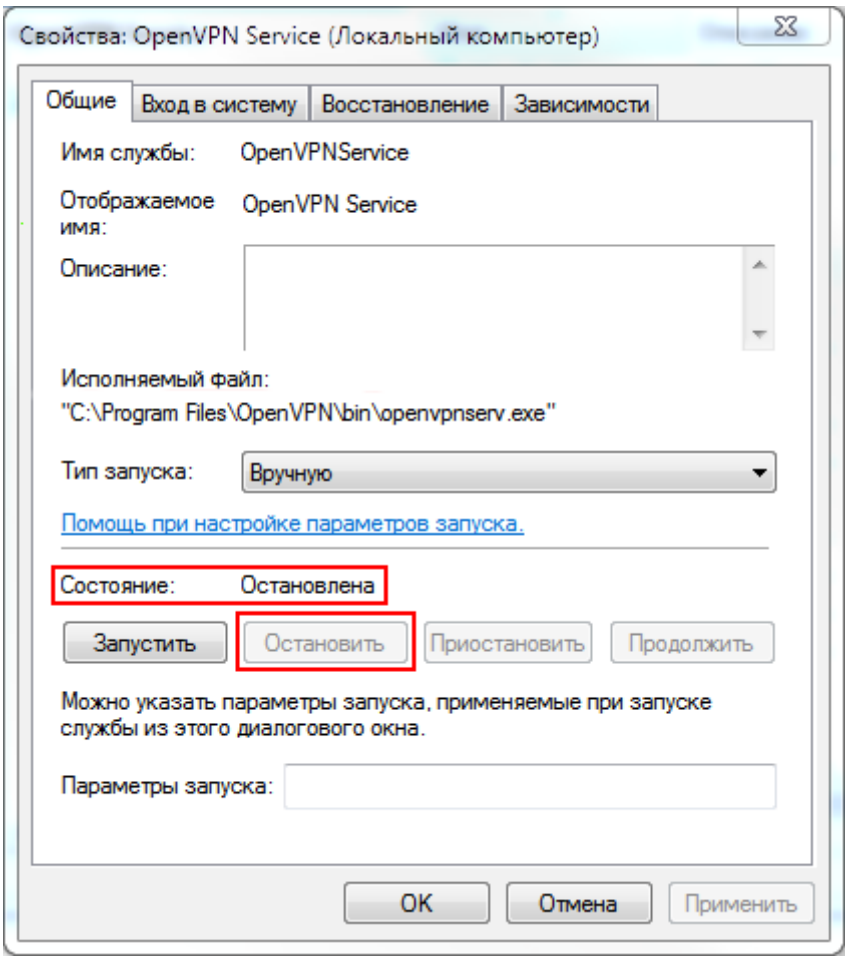
- Если у вас установлена версия 2.4.x, то необходимо скачать версию 2.4.6-xxxNN.

В результате вы должны получить архив (zip) обновленными исполнимыми файлами «OpenVPN».

5.2.4 Обновление файлов

5.2.4.1 Остановка работы «OpenVPN»

Если вы обновляете файлы на сервере «OpenVPN», то остановите работу службы «OpenVPN»: откройте окно свойств «OpenVPN Service» (как показано выше в пункте 5.2.1) и нажмите кнопку «Остановить». Проконтролируйте, что состояние службы изменилось на «Остановлено».



Внимание: после остановки службы «OpenVPN» контроллеры «БКД-ПК-RF» и «ECA Connect» не смогут подключаться и передавать данные на сервер информационной системы. Не забудьте запустить службу после окончания выполнения работ по обновлению!!!

Если вы обновляете файлы на клиенте «OpenVPN», то разорвите VPN соединение, если оно у вас установлено.

5.2.4.2 Резервное копирование файлов

Выполните резервную копию папки с исполнимыми файлами «OpenVPN». Создание резервной копии необходимо на случай возникновения проблем с запуском обновленной версии.

5.2.4.3 Резервное копирование файлов

Замените все файлы в папке с исполнимыми файлами «OpenVPN» на файлы из скачанного архива, утвердительно ответив на запрос о необходимости их замены.

5.2.4.4 Запуск

Если вы обновляете файлы на сервере «OpenVPN», то запустите работу службы «OpenVPN»: откройте окно свойств «OpenVPN Service» (как показано выше в пункте 5.2.1) и нажмите кнопку «Запустить». Проконтролируйте, что состояние службы изменилось на «Работает».