

УТВЕРЖДЕН
СЕИУ.00009-04 32 09 - ЛУ

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 3.0

Виртуальная частная сеть «OpenVPN-ГОСТ»

Руководство по использованию

СЕИУ.00009-04 32 09
Листов 131

Литера О

Аннотация

Настоящий документ содержит руководство по использованию виртуальной частной сети «OpenVPN-ГОСТ», которая представляет собой исполнение 7 (соответствует классу КС1) и исполнение 8 (соответствует классу КС2) СКЗИ «МагПро КриптоПакет» 3.0.

«МагПро» является зарегистрированной торговой маркой ООО «Криптоком».

Содержание

1	Назначение	7
2	Условия работы программы	8
3	Перечень функций	9
4	Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 3.0	10
5	Установка	11
5.1	УСТАНОВКА В LINUX (ИСПОЛЬЗОВАНИЕ ПАКЕТА RPM)	11
5.2	УСТАНОВКА В LINUX (БЕЗ RPM)	11
5.3	УСТАНОВКА В FreeBSD	11
5.4	УСТАНОВКА В WINDOWS	11
5.4.1	УСТАНОВКА ДЛЯ ЗАПУСКА ПОЛЬЗОВАТЕЛЯМИ, НЕ ИМЕЮЩИМИ АДМИНИСТРАТИВНЫХ ПРАВ	12
5.4.2	КОНТРОЛЬ НАД СЕРВИСОМ «OPENVPN-ГОСТ» ИЗ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА «OPENVPN-ГОСТ»	12
5.4.3	WINDOWS «RUN AS»	12
5.4.4	СОЗДАНИЕ ИКОНКИ RUN AS В ОС WINDOWS	13
6	Настройка	14
6.1	ОБЩИЕ ЗАМЕЧАНИЯ	14
6.2	ВЫБОР ТИПА VPN	14
6.2.1	МАРШРУТИЗИРОВАННАЯ VPN И VPN ТИПА «МОСТ»	14
6.2.2	НЕВОЗМОЖНОСТЬ РАБОТЫ «OPENVPN-ГОСТ» ПО ПРОТОКОЛУ UDP	15
6.2.3	НУМЕРАЦИЯ ЧАСТНЫХ ПОДСЕТЕЙ	15
6.3	ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ	16
6.3.1	ВВЕДЕНИЕ	16
6.3.2	ГЕНЕРАЦИЯ САМОПОДПИСАННОГО СЕРТИФИКАТА И КЛЮЧА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	17
6.3.3	ОТЗЫВ СЕРТИФИКАТОВ	17
6.4	КОНФИГУРАЦИОННЫЕ ФАЙЛЫ	18
6.4.1	ПОЛУЧЕНИЕ ПРИМЕРОВ КОНФИГУРАЦИОННЫХ ФАЙЛОВ	18
6.4.2	РЕДАКТИРОВАНИЕ СЕРВЕРНОГО КОНФИГУРАЦИОННОГО ФАЙЛА	18
6.4.3	РЕДАКТИРОВАНИЕ КЛИЕНТСКИХ КОНФИГУРАЦИОННЫХ ФАЙЛОВ	19
6.4.4	РАСШИРЕНИЕ ОБЛАСТИ ДЕЙСТВИЯ VPN С ВКЛЮЧЕНИЕМ ДОПОЛНИТЕЛЬНЫХ МАШИН В КЛИЕНТСКУЮ ИЛИ СЕРВЕРНУЮ ПРОДСЕТЬ	19
6.4.4.1	ВКЛЮЧЕНИЕ НЕСКОЛЬКИХ МАШИН СО СТОРОНЫ СЕРВЕРА ПРИ ИСПОЛЬЗОВАНИИ МАРШРУТИЗИРОВАННОЙ VPN (DEV TUN)	19
6.4.4.2	ВКЛЮЧЕНИЕ НЕСКОЛЬКИХ МАШИН НА СЕРВЕРНОЙ СТОРОНЕ ПРИ ИСПОЛЬЗОВАНИИ VPN ТИПА «МОСТ» (DEV TAP)	20
6.4.4.3	ВКЛЮЧЕНИЕ НЕСКОЛЬКИХ МАШИН НА КЛИЕНТСКОЙ СТОРОНЕ ПРИ ИСПОЛЬЗОВАНИИ МАРШРУТИЗИРОВАННОЙ VPN (DEV TUN)	20
6.4.4.4	ВКЛЮЧЕНИЕ НЕСКОЛЬКИХ МАШИН НА КЛИЕНТСКОЙ СТОРОНЕ ПРИ ИСПОЛЬЗОВАНИИ VPN ТИПА «МОСТ» (DEV TAP)	21

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6.4.5	Передача опций ДНСР клиентам	22
6.4.6	Конфигурирование клиент-специфичных правил и политик доступа	22
6.4.7	Использование альтернативных способов аутентификации	24
6.4.7.1	Использование скриптовых плагинов	24
6.4.7.2	Использование объектов общего доступа или DLL в качестве плагинов	24
6.4.7.3	Использование аутентификации по логину и паролю как единственной формы клиентской аутентификации	25
6.4.8	Добавление к конфигурации «OpenVPN-ГОСТ» двухфакторной аутентификации с использованием токенов на клиентской стороне	25
6.4.8.1	О двухфакторной аутентификации	25
6.4.8.2	Конфигурирование «OpenVPN-ГОСТ» для работы с токенами RUTOKEN	26
6.4.8.3	Конфигурирование «OpenVPN-ГОСТ» для работы с токенами Вьюга	26
6.4.9	Маршрутизация всего клиентского трафика (включая веб-трафик) через VPN	26
6.4.10	Маршрутизация всего клиентского трафика (включая веб-трафик) через VPN	26
6.4.10.1	Введение	26
6.4.10.2	Реализация	27
6.4.10.3	Предупреждения	27
6.4.11	Работа сервера «OpenVPN-ГОСТ» на динамическом IP-адресе	27
6.4.12	Подключение к серверу «OpenVPN-ГОСТ» через HTTP-прокси	28
6.4.13	Соединение с совместно используемым ресурсом SAMBA через «OpenVPN-ГОСТ»	29
6.4.14	Реализация конфигурации балансировки нагрузки/восстановления после сбоя	29
6.4.14.1	Клиент	29
6.4.14.2	Список серверов	30
6.4.14.3	Сервер	30
6.4.15	Конфигурирование «OpenVPN-ГОСТ» для автоматического запуска при старте системы	31
6.4.15.1	LINUX	31
6.4.15.2	WINDOWS	31
6.4.16	Запуск VPN и тест на начальную подключаемость	31
6.4.16.1	Запуск сервера	31
6.4.16.2	Запуск клиента	32
6.4.16.3	Поиск ошибок	32
7	Использование	34
7.1	Запуск на ОС семейства WINDOWS	34
7.2	Запуск на ОС, не входящих в семейство WINDOWS	34
7.3	Управление запущенным процессом «OpenVPN-ГОСТ»	34
7.3.1	Работа на LINUX/BSD/UNIX	34
7.3.2	Работа в WINDOWS в графическом интерфейсе	34
7.3.3	Работа в окне командной строки WINDOWS	35

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.4	РАБОТА В КАЧЕСТВЕ СЕРВИСА WINDOWS	35
7.3.5	МОДИФИКАЦИЯ КОНФИГУРАЦИИ ЗАПУЩЕННОГО СЕРВЕРА	35
7.3.6	ФАЙЛ СТАТУСА	35
7.3.7	ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА УПРАВЛЕНИЯ	36
7.3.7.1	КОМАНДА ECHO	36
7.3.7.2	КОМАНДА EXIT, QUIT	37
7.3.7.3	КОМАНДА HELP	37
7.3.7.4	КОМАНДА HOLD	37
7.3.7.5	КОМАНДА KILL	38
7.3.7.6	КОМАНДА LOG	38
7.3.7.7	КОМАНДА MUTE	38
7.3.7.8	КОМАНДА NET	38
7.3.7.9	КОМАНДА PASSWORD И USERNAME	39
7.3.7.10	КОМАНДА SIGNAL	39
7.3.7.11	КОМАНДА STATE	39
7.3.7.12	КОМАНДА STATUS	40
7.3.7.13	КОМАНДА USERNAME	40
7.3.7.14	КОМАНДА VERB	40
7.3.7.15	КОМАНДА VERSION	41
7.3.7.16	КОМАНДА AUTH-RETRY	41
7.3.7.17	ФОРМАТ СООБЩЕНИЙ В РЕАЛЬНОМ ВРЕМЕНИ	41
7.3.7.18	РАЗБОР КОМАНД	41
7.3.8	УПРАВЛЕНИЕ ПРОЦЕССОМ «OPENVPN-ГОСТ» С ПОМОЩЬЮ ИНТЕРФЕЙСА УПРАВЛЕНИЯ	42
7.4	УСИЛЕНИЕ БЕЗОПАСНОСТИ «OPENVPN-ГОСТ»	43
7.4.1	TLS-AUTH	43
7.4.2	USER/GROUP (КРОМЕ ОС WINDOWS)	44
7.4.3	НЕПРИВИЛЕГИРОВАННЫЙ РЕЖИМ (ТОЛЬКО В LINUX)	44
7.4.4	CHROOT (КРОМЕ ОС WINDOWS)	45
7.4.5	ХРАНЕНИЕ КОРНЕВОГО КЛЮЧА (CA.KEY) НА ОТДЕЛЬНОЙ МАШИНЕ БЕЗ СЕТЕВОГО СОЕДИНЕНИЯ	45
8	Приложение. Список опций команды openvpn	46
8.1	ОБЩИЕ ОПЦИИ	46
8.2	ТУННЕЛЬНЫЕ ОПЦИИ	46
8.3	СЕРВЕРНЫЙ РЕЖИМ	79
8.4	КЛИЕНТСКИЙ РЕЖИМ	91
8.5	ОПЦИИ ЗАШИФРОВАНИЯ КАНАЛА ДАННЫХ	94
8.6	ОПЦИИ РЕЖИМА TLS	101
8.7	ИНФОРМАЦИЯ ПО БИБЛИОТЕКЕ SSL	114
8.8	СОЗДАНИЕ СЛУЧАЙНОГО КЛЮЧА	114
8.9	РЕЖИМ КОНФИГУРАЦИИ СОХРАНЯЕМОГО ТУННЕЛЯ TUN/TAP	115
8.10	ОПЦИИ, СПЕЦИФИЧНЫЕ ДЛЯ WINDOWS	116
8.11	НЕЗАВИСИМЫЕ ОПЦИИ PKCS#11	122
8.12	СКРИПТОВАНИЕ И ПЕРЕМЕННЫЕ СРЕДЫ	122
8.12.1	Порядок выполнения скриптов	122
8.12.2	Типы и преобразование строк	123

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.12.3	ПЕРЕМЕННЫЕ СРЕДЫ	124
8.13	СИГНАЛЫ	130

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 Назначение

«МагПро КриптоПакет» 3.0 в исполнении «OpenVPN-ГОСТ» — полноценная виртуальная частная сеть (VPN) на основе TLS, которая реализует расширение сетевой безопасности слоя OSI 2 или 3 с использованием промышленного стандарта — протокола TLS, поддерживает гибкие способы криптографической аутентификации участников друг другом и позволяет использовать пользовательские или групповые политики контроля доступа с использованием правил межсетевого экрана, применимые к виртуальному интерфейсу VPN. «OpenVPN-ГОСТ» не является сетевым прокси-сервером и не работает через веб-браузер.

«OpenVPN-ГОСТ» предлагает масштабируемый режим клиент/сервер, позволяет нескольким клиентам подключаться к одному и тому же серверному процессу «OpenVPN-ГОСТ» через один TCP-порт.

«OpenVPN-ГОСТ» — это составная часть СКЗИ «МагПро КриптоПакет» 3.0, а именно исполнение 7 (соответствует классу КС1) и исполнение 8 (соответствует классу КС2) указанного СКЗИ.

«OpenVPN-ГОСТ» является функционально законченным изделием.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 Условия работы программы

«МагПро КриптоПакет» 3.0 в исполнении «OpenVPN-ГОСТ» предназначен для работы в следующих операционных системах:

Windows 7 SP1/8.1/10;

Windows Server 2008R2 SP1/2012/2012R2/2016

Debian GNU/Linux 7(wheezy)/8(jessie)/stretch;

Linux Mint 17.x, 18.x, Linux Mint Debian Edition 2

Ubuntu 14.04, 16.04;

RedHat Enterprise Linux 6, 7;

CentOS 6, 7;

SUSE Linux 11, 12;

OpenSUSE 42.2, 42.3;

OS EMIAS 1.0;

Альт Линукс 6, 7, 8;

МСВСфера Сервер 6.3, МСВСфера АРМ 6.3;

Атликс 3.1;

Гослинукс IC4;

FreeBSD 10.x, 11.x;

Oracle Solaris 10, 11;

MacOS 10.12;

Rosa Enterprise Desktop (RED) X2, X3;

Rosa Enterprise Linux Server (RELS) 6, 7; РОСА КОБАЛЬТ 1.0;

Astra Linux Special Edition РУСБ.10015-07.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 Перечень функций

«МагПро КриптоПакет» 3.0 в исполнении «OpenVPN-ГОСТ» реализует следующие функции:

- реализация протокола TLS с использованием российских наборов алгоритмов шифрования TLS_GOSTR341112_256_WITH_28147_CNT_IMIT и TLS_GOSTR341001_WITH_28147_CNT_IMIT (набор TLS_GOSTR341001_WITH_28147_CNT_IMIT следует использовать только для соединения с серверами, не поддерживающими набор TLS_GOSTR341112_256_WITH_28147_CNT_IMIT);
- шифрование и имитозащита в соответствии с ГОСТ 28147-89 и HMAC ГОСТ Р 34.11 данных, передаваемых по сети;
- вычисления ключа парной связи по алгоритму VKO с использованием как долговременных, так и эфемерных пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10;
- формирование эфемерных ключевых пар в соответствии с ГОСТ Р 34.10;
- формирования производных сеансовых ключей.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 3.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 3.0 осуществляется в строгом соответствии с требованиями документа «СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «МАГПРО КРИПТОПАКЕТ» 3.0. ПРАВИЛА ПОЛЬЗОВАНИЯ» (СЕИУ.СЕИУ.00009–04 94).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 Установка

Исполняемые файлы «OpenVPN-ГОСТ» следует установить и на клиентской, и на серверной машинах, потому что одни и те же исполняемые файлы предоставляют и клиентские, и серверные функции.

5.1 Установка в Linux (использование пакета RPM)

Если вы пользуетесь дистрибутивом Linux, который поддерживает пакеты RPM (SuSE, Fedora, Redhat, и т.д.), следует инсталлировать «OpenVPN-ГОСТ» с использованием этого механизма. Для этого необходимо воспользоваться существующим бинарным файлом RPM для вашего дистрибутива. Имея файл .rpm, вы можете установить его с помощью обычной команды

```
rpm -ivh openvpn-2.1_i386.rpm
```

или

```
rpm -ivh openvpn-2.1_x86_64.rpm
```

или обновить существующую установку с помощью

```
rpm -Uvh openvpn-2.1_i386.rpm.rpm
```

или

```
rpm -Uvh openvpn-2.1_x86_64.rpm
```

Установка «OpenVPN-ГОСТ» из бинарного пакета RPM имеет три зависимости:

- openssl
- lzo
- pam

5.2 Установка в Linux (без RPM)

Если вы пользуетесь Debian или дистрибутивом Linux, не основанным на RPM, воспользуйтесь пакетным механизмом, специфичным для вашего дистрибутива, таким как apt-get для Debian.

5.3 Установка в FreeBSD

Установка «OpenVPN-ГОСТ» на данном типе системы осуществляется путем установки бинарных пакетов.

5.4 Установка в Windows

«OpenVPN-ГОСТ» должна быть установлена и запущена пользователем, имеющим административные привилегии (это ограничение определяется Windows, а не «OpenVPN-ГОСТ»). Это ограничение можно обойти, запуская «OpenVPN-ГОСТ» в фоновом режиме как сервис, в этом случае даже не имеющие прав администратора пользователи смогут иметь доступ к VPN, когда она будет установлена.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5.4.1 Установка для запуска пользователями, не имеющими административных прав

В установочный пакет «OpenVPN-ГОСТ» включена небольшая сервисная оболочка. Этот сервис просто запускает все конфигурационные файлы, которые находит в каталоге OpenVPN\config. Если вы хотите, чтобы ваш туннель «OpenVPN-ГОСТ» работал всегда, вне зависимости от того, вошли вы в систему или нет, вы можете просто сконфигурировать сервис «OpenVPN-ГОСТ» автоматически запускаться при запуске Windows. Но может быть, удобнее запускать и выключать туннель по желанию, что можно делать, запуская и выключая сервис.

Крупный недостаток этого способа заключается в том, что нет возможности предоставить службе «OpenVPN-ГОСТ» пароль, который был применен для зашифрования вашего закрытого ключа. Это значит, что вы должны использовать незашифрованный закрытый ключ.

Как правило, запуск и остановка сервиса требуют прав администратора, но вы можете дать обычному пользователю право контролировать индивидуальный сервис. Это делается с помощью утилиты subinacl.exe, включенной в Windows Resource Kit.

Чтобы предоставить пользователю John право запускать и выключать сервис «OpenVPN-ГОСТ», войдите в систему с правами администратора и выполните следующую команду:

```
subinacl /SERVICE "OpenVPNService" /GRANT=john=TO
```

5.4.2 Контроль над сервисом «OpenVPN-ГОСТ» из графического интерфейса «OpenVPN-ГОСТ»

Умолчательная установка графического интерфейса «OpenVPN-ГОСТ» не дает вам возможности контролировать сервис «OpenVPN-ГОСТ». Существуют два способа это сделать. Если вы работаете как администратор, и просто хотите удобный способ контролировать сервис «OpenVPN-ГОСТ», вы можете делать это через скрытое меню. Для этого необходимо установить следующее значение регистра в 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN-GUI\allow_service
```

Существует специальный режим «Только сервис», подходящий для пользователей, работающих без прав администратора. Этот режим меняет поведение действий Connect и Disconnect таким образом, что они запускают и останавливают сервис «OpenVPN-ГОСТ» вместо прямого запуска openvpn.exe, как обычно. Он также прячет меню «Настройка прокси», поскольку оно не влияет на сервис. Чтобы запустить этот режим, установите следующее значение регистра в 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN-GUI\service_only
```

Также помните, что обычный пользователь не имеет прав записи в каталог OpenVPN\config, поэтому он не сможет редактировать конфигурационный файл «OpenVPN-ГОСТ» или менять свой пароль, если вы не дадите ему права на запись в эти файлы. Чтобы спрятать эти пункты меню, установите следующие значения регистра в 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN-GUI\allow_edit
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN-GUI\allow_password
```

5.4.3 Windows «Run as»

Начиная с Windows 2000, существует возможность запустить приложение от лица другого пользователя, нежели вошедший в систему. Лучший способ использовать эту возможность в

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

данном случае — запустив графический интерфейс «OpenVPN-ГОСТ» . Поскольку графический интерфейс работает от лица администратора, то пока он работает, может быть открыто и закрыто любое количество туннелей «OpenVPN-ГОСТ» .

Помните, что, используя эту возможность, вы даете пользователям возможность расширить свои права до административных. Если вы не хотите, чтобы компьютер работал под администратором, для того, чтобы защититься от вредоносного кода из сети, выполняющегося с правами администратора, то это может быть хороший способ, но если вашим пользователям ни при каких обстоятельствах нельзя запускать приложения с правами администратора, вы НЕ должны использовать этот способ работы с графическим интерфейсом «OpenVPN-ГОСТ» !

Устанавливая графический интерфейс, обязательно отключите опцию AutoStart OpenVPN GUI, поскольку вам понадобится создавать иконку для запуска вручную.

5.4.4 Создание иконки Run As в ОС Windows

- Создайте обычную иконку для openvpn-gui.exe (c:\program files\openvpn\bin\openvpn-gui.exe) на рабочем столе.
- Щелкните правой клавишей мыши по иконке и выберите Свойства.
- Щелкните на Advanced...
- Поставьте галочку Run with different credentials.

Когда вы щелкаете двойным щелчком мыши по этой иконке, появится окно, в котором нужно будет ввести логин и пароль для пользователя, от лица которого вы хотите запустить графический интерфейс. Если вы хотите, чтобы он запускался автоматически, когда вы входите в систему, перенесите эту иконку в каталог Startup в меню Start-Programs. Тогда у вас будут запрашивать логин и пароль непосредственно каждый раз при входе в систему.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6 Настройка

6.1 Общие замечания

Для настройки «OpenVPN-ГОСТ» необходимо:

- Определиться с типом VPN — выбрать маршрутизированную VPN или VPN типа «мост» (см. раздел 6.2).
- Создать или воспользоваться инфраструктурой открытых ключей для создания сертификата закрытого ключа сервера и каждого клиента, корневого сертификата удостоверяющего центра и ключа, который используется для подписи каждого из серверных и клиентских сертификатов (см. раздел 6.3.1).
- Создать конфигурационные файлы для сервера и клиентов (см. раздел 6.4).

6.2 Выбор типа VPN

6.2.1 Маршрутизированная VPN И VPN типа «мост»

Маршрутизирование и связь типа «мост» (бриджинг) - два способа связи систем через VPN.

Когда клиент подключается к удаленной сети через VPN типа «мост», ему присваивается IP-адрес, являющийся частью удаленной физической подсети Ethernet, и после этого он может взаимодействовать с другими машинами удаленной сети, как будто они соединены локально. Настройки VPN типа «мост» требуют специального инструмента, зависящего от операционной системы, чтобы связать адаптер подсети Ethernet с виртуальным устройством стиля TAP. Например, для Linux такой инструмент - brctl. На ОС семейства Windows выберите адаптер TAP-Win32 и адаптер сети Ethernet в Control Panel->Network connections, затем щелкните правой клавишей мыши и выберите Bridge Connections.

Когда клиент подключается через маршрутизированную VPN, он использует собственную отдельную подсеть, и маршруты устанавливаются и на клиентской машине и на удаленном гейте, чтобы пакеты данных беспрепятственно проходили через VPN. Здесь клиент - обязательно одна машина, это может быть подсеть из нескольких машин.

Маршрутизация и связь типа «мост» с функциональной точки зрения очень похоже, с важным различием в том, что маршрутизированная VPN не пропускает широковещательные рассылки IP-пакетов, а VPN типа «мост» пропускает.

Эти разновидности VPN связаны с использованием различных адаптеров. Устройство TAP - виртуальный адаптер сети Ethernet, устройство TUN - виртуальная IP-связь точка-в-точку.

Когда вы используете VPN типа «мост», вы должны всегда использовать -dev tap на обоих концах соединения. Если вы используете маршрутизированную VPN, вы можете использовать и -dev tap, и -dev tun, но вы должны использовать одно и то же на обоих концах соединения. -dev tun немного более эффективный вариант для случая маршрутизации.

Преимущества VPN типа «мост»:

- Широковещательные рассылки IP-пакетов проходят через VPN - это позволяет программному обеспечению, зависящему от рассылок локальной сети, например, Windows NetBIOS, обмениваться файлами и просматривать сетевое окружение.
- Не нужно конфигурировать маршрутизационных утверждений.
- Работает с любым протоколом, который может функционировать в сети Ethernet, включая IPv4, IPv6, Netware IPX, AppleTalk, etc.
- Решение, относительно легкое для конфигурирования.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Недостатки VPN типа «мост»:

- Менее эффективна, чем маршрутизирование, и плохо масштабируется.

Преимущества маршрутизированной VPN:

- Эффективность и масштабируемость
- Позволяет лучшую настройку MTU для эффективности.

Недостатки маршрутизированной VPN:

- Клиенты должны использовать сервер WINS (например, Samba), чтобы позволить работать просмотру сети через VPN.
- Необходимо настроить маршруты, связывающие каждую подсеть.
- Программное обеспечение, зависящее от бродкастов, не будет «видеть» машины на другой стороне VPN.
- Работает в основном только с IPv4, и с IPv6 в случаях, когда драйверы tun на обоих концах соединения эффективно поддерживают его.

В общем, маршрутизирование, вероятно, лучший выбор для большинства пользователей, потому что оно более эффективно и его легче настроить (как и саму конфигурацию «OpenVPN-ГОСТ»). Маршрутизирование также предоставляет большую возможность избирательно контролировать права доступа на клиентски-специфичной основе.

Рекомендуется использовать маршрутизацию, если только вам не нужны специфические возможности, требующие использования «моста», такие как:

1. VPN должна работать с не-IP протоколами, такими как IPX
2. Вы запускаете приложения над VPN, которые полагаются на сетевую ретрансляцию (такие как сетевые игры)
3. Вы бы хотели позволить просматривать через VPN совместно используемые ресурсы, не устанавливая серверы Samba или WINS.

6.2.2 Невозможность работы «OpenVPN-ГОСТ» по протоколу UDP

Следует принять во внимание, что в силу специфики RFC4357 (<http://www.ietf.org/rfc/rfc4357.txt>) данная реализация «OpenVPN-ГОСТ» (в целом, как и любая другая реализация «OpenVPN-ГОСТ»), не будет работать по UDP.

6.2.3 Нумерация частных подсетей

Установка VPN часто требует связывания вместе частных подсетей из разных локаций.

IANA зарезервировала следующие три блока пространства IP-адресов для частных сетей (кодифицировано в RFC 1918):

10.0.0.0 10.255.255.255 (префикс 10/8)

172.16.0.0 172.31.255.255 (префикс 172.16/12)

192.168.0.0 192.168.255.255 (префикс 192.168/16)

В то время как адреса из этих блоков следует в норме использовать в конфигурациях VPN, важно выбирать адреса, которые минимизируют возможность конфликтов IP-адресов или подсетей. Типы конфликтов, которых следует избегать:

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

- Конфликты разных мест в VPN, использующих одинаковую нумерацию подсетей LAN;
- Соединения удаленного доступа из мест, которые используют частные подсети, конфликтующие с вашими подсетями VPN.

Например, предположим, что вы используете популярную подсеть 192.168.0.0/24 как вашу частную подсеть LAN. Теперь вы пытаетесь соединиться с VPN из интернет-кафе, использующего ту же подсеть для своего WiFi LAN. У вас будет проблема маршрутизации, потому что ваша машина не поймет, относится ли 192.168.0.1 к локальному WiFi-гейту или к тому же адресу на VPN.

В качестве другого примера, предположим, что вы хотите соединить вместе несколько точек с помощью VPN, но каждая точка использует 192.168.0.0/24 в качестве своей подсети LAN. Это не будет работать, если не добавить дополнительный слой трансляции NAT, потому что VPN не поймет, как маршрутизировать пакеты между несколькими точками, если эти точки не используют подсеть, которая уникально идентифицирует их.

Лучшее решение — избегать пользоваться 10.0.0.0/24 или 192.168.0.0/24 в качестве сетевых адресов LAN. Вместо этого используйте что-нибудь, что с более низкой вероятностью будет использовано в WiFi-кафе, аэропорту или отеле, откуда вы, возможно, захотите установить удаленный доступ. Лучшие кандидаты — подсети в середине большого блока 10.0.0.0/8 (например, 10.66.77.0/24).

Чтобы избежать кросс-локационных конфликтов номеров IP, всегда используйте уникальную нумерацию для ваших подсетей LAN.

6.3 Инфраструктура открытых ключей

6.3.1 Введение

Инфраструктура открытых ключей (PKI) состоит из:

- Отдельного сертификата (также известного как открытый ключ) и закрытого ключа для сервера и каждого клиента, и
- Корневого сертификата удостоверяющего центра и ключа, который используется для подписи каждого из серверных и клиентских сертификатов.

Для аутентификации необходимо, чтобы клиент мог аутентифицировать сервер по его сертификату. Дополнительно можно сделать так, чтобы сервер мог аутентифицировать клиентов по их сертификатам. «OpenVPN-ГОСТ» поддерживает такую двунаправленную аутентификацию, что означает, что клиент должен аутентифицировать серверный сертификат, и сервер должен аутентифицировать клиентский сертификат, прежде чем устанавливается взаимное доверие.

И сервер, и клиент будут аутентифицировать друг друга, сначала проверив, что представленный кандидат был подписан на сертификате удостоверяющего центра, а затем тестируя информацию в заголовке уже аутентифицированного сертификата, такую, как common name сертификата или его тип (клиентский или серверный).

Эта модель безопасности имеет ряд желательных признаков с точки зрения VPN:

- Серверу нужен только его собственный сертификат/ключ — ему не нужно знать индивидуальные сертификаты всех клиентов, которые, возможно, установят с ним соединение.
- Сервер будет принимать только клиентов, чьи сертификаты были подписаны на сертификате удостоверяющего центра (который будет генерирован ниже). И поскольку сервер может выполнять эту проверку подписи без необходимости доступа к самому закрытому ключу УЦ, ключ УЦ (самый чувствительный ключ во всей PKI) может находиться на совершенно другой машине, даже на машине без сетевого соединения.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

- Если закрытый ключ скомпрометирован, он может быть деактивирован путем добавления его сертификата в CRL (список отзыва сертификатов). CRL позволяет скомпрометированным сертификатам быть отвергнутыми избирательно, не требуя перестраивать всю PKI.
- Сервер может усилить клиентски-специфичные права доступа, основанные на внутренних полях сертификата, таких как Common Name.

Обратите внимание, что часы сервера и клиента должны быть более-менее синхронизированы, иначе сертификаты могут работать некорректно.

6.3.2 Генерация самоподписанного сертификата и ключа удостоверяющего центра

Для генерации комплекта ключей и сертификатов, необходимых для работы OpenVPN-ГОСТ, рекомендуем использовать набор утилит `easy-gost`, поставляемый в составе дистрибутива.

6.3.3 Отзыв сертификатов

Отзыв сертификата означает объявление недействительным ранее подписанного сертификата, так что его больше нельзя использовать для целей аутентификации.

Типичные причины желаяния отозвать сертификат включают:

- Закрытый ключ, связанный с сертификатом, скомпрометирован или украден.
- Пользователь зашифрованного закрытого ключа забывает пароль к ключу.
- Вы хотите прекратить доступ пользователя к VPN.

Сначала вам нужно создать список отзыва. Хорошая практика — создать пустой список отзыва, и пусть ваши клиенты его проверяют. Таким образом, когда вам действительно придется отзываться сертификат, у вас не будет проблем с тем, чтобы заставить клиентов это заметить.

Чтобы создать список отзыва для вашего УЦ, вам прежде всего нужно создать файл `index.txt`. Это сначала будет пустой файл (созданный командой `touch`). Однако, когда вы начнете отзываться сертификаты, в него будет добавляться информация. Файл читабелен для людей и неподписан, поэтому нам нужно, чтобы OpenSSL сделала для него подписанную PEM-форму. Таким образом, когда вы получите свой пустой файл указателя, вы можете сделать из него список отзыва с помощью:

```
openssl ca -gencrl -keyfile ca.key -cert ca.crt -out crl.pem
```

где `ca.key` --- закрытый ключ CA

`ca.crt` --- сертификат CA

`crl.pem` --- требуемый файл, содержащий списки отзыва

Эта команда создаст для вас список отзыва, действительный в течение умолчательного промежутка времени (1 месяц). В том случае, если список отзыва используется только на серверах, которые вы контролируете, и где вы уверены, что обновите список отзыва при следующем отзыве, вы, возможно, захотите увеличить время жизни списка отзыва. Иначе через несколько месяцев ваши серверы будут жаловаться, что список отзыва устарел.

Чтобы увеличить продолжительность времени, в течение которого список отзыва действителен, добавьте опцию `crl days xxx` к вышеприведенной команде генерации списка отзыва (где `xxx` — количество дней, в течение которых список отзыва действителен)

Примечание. Если срок действия вашего списка отзыва истекает, прежде чем вы отзовете сертификат, просто создайте новый, как описано выше. Список отзыва — просто подписанная

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

копия внутреннего списка отозванных сертификатов, имеющая срок действия и оформленная в стандартном формате. Вы можете создавать новые списки отзыва, когда захотите.

Теперь, когда начальный список отзыва готов, мы отзовем сертификат:

```
openssl ca -revoke bad.crt -keyfile ca.key -cert ca.crt
```

где `ca.key` и `ca.crt` --- то же самое, что и в предыдущей команде, а `bad.crt` --- отзываемый сертификат.

Это автоматически обновит ваш файл `index.txt`, добавив новые детали об отозванном сертификате. Теперь вам нужно создать новый файл списка отзыва той же командой, которой мы пользовались выше, чтобы создать пустой файл. Когда новый список отзыва создан, его необходимо опубликовать!

Если вы хотите поиграть с продолжительностью действия списка отзыва и прочими подобными вещами, вам необходимо прочитать раздел «Опции списка отзыва» в руководстве по OpenSSL CA. Если вы хотите манипулировать со списком отзыва, просматривать его и т.д., прочитайте руководство по утилите CRL.

6.4 Конфигурационные файлы

6.4.1 Получение примеров конфигурационных файлов

Лучше всего использовать готовые примеры конфигурационных файлов «OpenVPN-ГОСТ» в качестве старта для вашей собственной конфигурации. Эти файлы можно найти в:

(В Windows) `C:\Program Files\OpenVPN\sample-config`

(В Linux) `/etc/openvpn-gost/`

(В FreeBSD) `/usr/local/openvpn-gost/etc`

(В MacOS) `/opt/openvpn-gost/etc`

Обратите внимание что в Linux, BSD или Unix-подобных операционных системах примеры конфигурационных файлов называются `gost-server.conf.sample` и `client.conf.sample`. В Windows они называются `gost-server.ovpn` и `gost-client.ovpn`.

6.4.2 Редактирование серверного конфигурационного файла

Пример серверного конфигурационного файла — идеальная стартовая точка для серверной конфигурации «OpenVPN-ГОСТ». Он создаст VPN с использованием виртуального сетевого интерфейса, будет слушать клиентские соединения на tcp-порту 1194 (номер порта, зарезервированный для VPN), и будет распределять виртуальные адреса для подключающихся клиентов из подсети 10.9.1.0/24.

Прежде чем использовать пример конфигурационного файла, вам прежде всего следует отредактировать параметры `ca`, `cert` и `key` так, чтобы они указывали на файлы, которые вы сгенерировали раньше.

Теперь конфигурацию сервера можно использовать, но вы можете захотеть ее еще больше модифицировать.

1. Если вы используете VPN типа «мост», вы должны использовать `server-bridge` вместо `server` и `dev tap`.
2. Если вы хотите использовать другой набор виртуальных IP-адресов, нежели 10.9.1.0/24, вам следует модифицировать директиву `server`. Помните, что этот набор виртуальных адресов должен быть частным набором, который не используется в вашей сети.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Добавьте директиву `client-to-client`, если вы хотите, чтобы подключающиеся клиенты могли видеть друг друга через VPN. По умолчанию клиенты могут видеть только сервер.
4. Если вы используете Windows, необходимо закомментировать директивы `user nobody` и `group nobody`.

Если вы хотите запустить несколько экземпляров «OpenVPN-ГОСТ» на одной и той же машине, каждый со своим конфигурационным файлом, это возможно если вы:

1. используете отдельный номер порта для каждого экземпляра.
2. Если вы используете Windows, каждая конфигурация «OpenVPN-ГОСТ» должна использовать свой собственный адаптер TAP-Win32. Вы можете добавить дополнительные адаптеры в Start Menu -> All Programs -> «OpenVPN-ГОСТ» -> Add a new TAP-Win32 virtual ethernet adapter.
3. Если вы запускаете несколько экземпляров «OpenVPN-ГОСТ» из одного и того же каталога, обязательно отредактируйте директивы, которые создают выходные файлы, чтобы различные экземпляры не переписывали выходные файлы друг друга. Эти директивы включают `log`, `log-append` и `status`.

6.4.3 Редактирование клиентских конфигурационных файлов

Пример клиентской конфигурации (`client.conf.sample` на Linux/BSD/MacOS или `gost-client.ovpn` на Windows) отражает умолчательные директивы, установленные в примере серверного конфигурационного файла.

1. Как и с серверным конфигурационным файлом, сначала отредактируйте параметры `ca`, `cert` и `key` так, чтобы они указывали на файлы, которые вы создали раньше. Обратите внимание, что каждый клиент должен иметь свою собственную пару `cert/key`. Только файл `ca` универсален для сервера «OpenVPN-ГОСТ» и всех клиентов.
2. Далее, отредактируйте директиву `remote` так, чтобы она указывала на `hostname/IP-адрес` и номер порта сервера «OpenVPN-ГОСТ» (если ваш сервер «OpenVPN-ГОСТ» будет работать на машине с одним сетевым адаптером за брандмауэром/NAT-гейтом, используйте публичный IP-адрес гейта и номер порта, который вы сконфигурировали для гейта для форвардинга на сервер «OpenVPN-ГОСТ»).
3. Наконец, убедитесь, что клиентский конфигурационный файл соответствует директивам в серверном конфигурационном файле. Самое главное — проверить, что директивы `dev` (`tun` или `tap`) и `proto` (`tcp`) совпадают. Также убедитесь, что `comp-lzo` и `fragment`, если используются, присутствуют и в серверном, и в клиентском конфигурационном файле.

6.4.4 Расширение области действия VPN с включением дополнительных машин в клиентскую или серверную подсеть

6.4.4.1 Включение нескольких машин со стороны сервера при использовании маршрутизированной VPN (`dev tun`)

Поскольку VPN работает в режиме «точка-точка» между клиентом и сервером, может быть желательно расширить область действия VPN так, чтобы клиенты могли связаться с несколькими машинами в сети сервера, а не только с самой машиной сервера.

Для целей этого примера предположим, что серверная LAN использует подсеть `10.66.0.0/24`, а множество IP-адресов VPN использует `10.9.1.0/24`, как показано в директиве `server` в конфигурационном файле сервера «OpenVPN-ГОСТ» .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Сначала вы должны *объявить* подсеть 10.66.0.0/24 клиентам VPN как доступную через VPN. Это легко делается с помощью следующей директивы серверного конфигурационного файла:

```
push "route 10.66.0.0 255.255.255.0"
```

Затем вы должны установить маршрут на гейте серверной LAN, чтобы маршрутизировать подсеть клиента VPN (10.9.1.0/24) на сервер «OpenVPN-ГОСТ» (это необходимо только в том случае, если сервер «OpenVPN-ГОСТ» и гейт LAN — различные машины.)

Убедитесь, что вы включили форвардинг IP и TUN/TAP на серверной машине «OpenVPN-ГОСТ» .

6.4.4.2 Включение нескольких машин на серверной стороне при использовании VPN типа «мост» (dev tap)

Одно из преимуществ использования VPN типа «мост» через Ethernet заключается в том, что это вы получаете без дополнительного конфигурирования.

6.4.4.3 Включение нескольких машин на клиентской стороне при использовании маршрутизированной VPN (dev tun)

В типичном сценарии удаленного доступа клиентская машина подключается к VPN как одиночная машина. Но предположим, что клиентская машина — гейт локальной сети (например, домашнего офиса), и вы бы хотели, чтобы все машины клиентской сети могли подключаться к VPN.

Для этого примера предположим, что клиентская локальная сеть использует подсеть 192.168.4.0/24, а клиент VPN использует сертификат с Common Name client2. Наша цель — так настроить VPN, чтобы любая машина клиентской сети могла общаться с любой машиной серверной сети через VPN.

Перед настройкой необходимо обеспечить несколько основных требований:

- Клиентская локальная подсеть (в нашем примере 192.168.4.0/24) не должна экспортироваться в VPN сервером или любыми другими клиентскими локациями, которые используют ту же подсеть. Каждая подсеть, объединенная VPN через маршрутизацию, должна быть уникальной.
- Клиент должен иметь уникальное поле Common Name в своем сертификате (в нашем примере client2), и флаг duplicate-cn не должен использоваться в серверном конфигурационном файле «OpenVPN-ГОСТ» .

Прежде всего убедитесь, что на клиентской машине включен форвардинг IP и TUN/TAP.

Далее мы произведем необходимые конфигурационные изменения на серверной стороне. Если серверный конфигурационный файл не указывает на каталог клиентской конфигурации, добавьте указание сейчас:

```
client-config-dir ccd
```

В вышеуказанной директиве ccd должен быть именем каталога, который был заранее создан в каталоге по умолчанию, где работает серверный демон «OpenVPN-ГОСТ» . В Linux это обычно /etc/openvpn, а в Windows \Program Files\OpenVPN\config. Когда новый клиент связывается с сервером «OpenVPN-ГОСТ» , демон просканирует этот каталог в поисках файла, который соответствует полю common name соединяющегося клиента. Если соответствующий

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

файл найден, он будет прочитан и обработан для применения дополнительных директив конфигурационного файла к поименованному клиенту.

Следующий шаг — создать файл под названием `client2` в каталоге `ccd`. Этот файл должен содержать строку:

```
iroute 192.168.4.0 255.255.255.0
```

Это скажет серверу «OpenVPN-ГОСТ», что подсеть `192.168.4.0/24` следует маршрутизировать на `client2`.

Далее, добавьте следующую строку к главному серверному конфигурационному файлу (а не к файлу `ccd/client2`):

```
route 192.168.4.0 255.255.255.0
```

Вы можете спросить, почему используются и `route`, и `iroute`? Причина в том, что `route` контролирует маршрутизацию из ядра на сервер «OpenVPN-ГОСТ» (через интерфейс TUN), а `iroute` контролирует маршрутизацию от сервера «OpenVPN-ГОСТ» к удаленным клиентам. Оба необходимы.

Далее, спросите себя, хотите ли вы допустить сетевую передачу информации между подсетью `client2` (`192.168.4.0/24`) и другими клиентами сервера «OpenVPN-ГОСТ». Если да, добавьте к серверному конфигурационному файлу следующее:

```
client-to-client
push "route 192.168.4.0 255.255.255.0"
```

Это заставит сервер «OpenVPN-ГОСТ» *объявить* подсеть `client2` остальным подключающимся клиентам.

Последний шаг, который часто забывают — добавить маршрут к гейту серверной локальной сети, который направляет `192.168.4.0/24` к серверу «OpenVPN-ГОСТ» (вам это не понадобится, если сервер «OpenVPN-ГОСТ» - гейт для сервера локальной сети). Предположим, что вы пропустили этот шаг и попытались передать сигнал ring машине (не самому серверу «OpenVPN-ГОСТ») в серверной сети из `192.168.4.8`. Внешний сигнал, вероятно, достигнет машины, но она не будет знать, как маршрутизировать ответный сигнал, потому что не будет знать, как достичь `192.168.4.0/24`. Основное правило пользования состоит в том, что когда вы маршрутизируете целые локальные сети через VPN (где сервер VPN — не та же машина, что гейт локальной сети), убедитесь, что гейт локальной сети маршрутизирует все подсети VPN на серверную машину VPN.

Подобным же образом, если клиентская машина, на которой работает «OpenVPN-ГОСТ», не является гейтом клиентской локальной сети, то гейт клиентской локальной сети должен иметь маршрут, который направляет все подсети, которые можно видеть через VPN, на клиентскую машину «OpenVPN-ГОСТ».

6.4.4.4 Включение нескольких машин на клиентской стороне при использовании VPN типа «мост» (dev tap)

Это требует более сложной настройки (может быть, не сложнее на практике, но сложнее для объяснения в деталях):

- Необходимо соединить клиентский интерфейс TAP с сетевым адаптером, соединенным с локальной сетью на клиенте, в режиме «мост».
- Необходимо вручную установить IP/маску сети на интерфейсе TAP на клиенте.
- Необходимо сконфигурировать машины на клиентской стороне так, чтобы они использовали IP/маску сети, которая находится внутри подсети, соединенной в режиме «мост», возможно, запрашивая сервер DHCP на стороне сервера «OpenVPN-ГОСТ» в VPN.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6.4.5 Передача опций DHCP клиентам

Сервер «OpenVPN-ГОСТ» может передавать опции DHCP, такие как адреса серверов DNS и WINS, клиентам. Клиенты Windows могут принимать переданные опции DHCP сами по себе, а клиенты других операционных систем могут их принимать, используя скрипт `ip` на клиентской стороне, который анализирует список переменных среды `foreign_option_n`.

Например, предположим, что вы бы хотели, чтобы соединяющиеся клиенты использовали внутренний DNS-сервер на 10.66.0.4 или 10.66.0.5 и сервер WINS на 10.66.0.8. Добавьте в конфигурацию сервера «OpenVPN-ГОСТ» :

```
push "dhcp-option DNS 10.66.0.4"
push "dhcp-option DNS 10.66.0.5"
push "dhcp-option WINS 10.66.0.8"
```

Чтобы протестировать эту возможность на Windows, запустите следующую команду из окна командной строки после того, как машина подключилась к серверу «OpenVPN-ГОСТ» :

```
ipconfig /all
```

Запись для адаптера TAP-Win32 должна показать опции DHCP, переданные сервером.

6.4.6 Конфигурирование клиент-специфичных правил и политик доступа

Предположим, что мы настраиваем VPN для компании, и нам бы хотелось установить различные политики доступа для 3 различных классов пользователей:

- Системные администраторы — полный доступ ко всем машинам сети
- Сотрудники — доступ только к серверам Samba/email
- Контрактеры — доступ только к специальному серверу

Базовый подход, который мы предпримем:

1. выделить каждому классу собственный диапазон IP-адресов,
2. контролировать доступ к машинам, установив брандмауэрные правила, которые основываются на виртуальном IP-адресе клиента.

В нашем примере, предположим, что у нас меняется количество сотрудников, но только один системный администратор и два контрактора. Наш подход к распределению IP будет состоять в том, чтобы поместить всех сотрудников в диапазон IP-адресов, а потом выдать фиксированные IP-адреса системному администратору и контракторам.

Заметьте, что одно из требований к этому примеру заключается в том, что у вас есть программный брандмауэр, работающий на серверной машине «OpenVPN-ГОСТ», который дает вам возможность задавать конкретные брандмауэрные правила. Для нашего примера мы предположим, что этот брандмауэр - iptables в Linux.

Сначала создадим карту виртуальных IP-адресов в соответствии с каждым классом:

Класс	Диапазон виртуальных IP	Позволенный доступ к локальной сети	Поля common name
Сотрудники	10.8.0.0/24	Сервер samba/email на 10.66.4.4	[различные]
Системные администраторы	10.8.1.0/24	Вся подсеть 10.66.4.0/24	sysadmin1

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Контракторы 10.8.2.0/24 Сервер контракторов contractor1,
на 10.66.4.12 contractor2

Теперь переведем эту карту в серверную конфигурацию «OpenVPN-ГОСТ». Прежде всего убедитесь, что вы выполнили вышеописанные шаги, сделав подсеть 10.66.4.0/24 доступной для всех клиентов (хотя мы сконфигурируем маршрутизацию так, чтобы позволить клиентский доступ ко всей подсети 10.66.4.0/24, затем мы наложим ограничения доступа, пользуясь брандмауэрными правилами, чтобы реализовать вышеприведенную таблицу политик).

Прежде всего определим статический номер для нашего интерфейса tun, чтобы мы могли позже сослаться на него в наших брандмауэрных правилах:

```
dev tun0
```

В серверном конфигурационном файле определим диапазон IP-адресов для сотрудников:

```
server 10.8.0.0 255.255.255.0
```

Добавим маршруты для диапазонов системного администратора и контракторов:

```
route 10.8.1.0 255.255.255.0
```

```
route 10.8.2.0 255.255.255.0
```

Поскольку мы будем присваивать фиксированные IP-адреса специфичным системным администраторам и контракторам, мы будем пользоваться каталогом клиентской конфигурации:

```
client-config-dir ccd
```

Теперь поместите специальные конфигурационные файлы в подкаталог ccd, чтобы определить фиксированный IP-адрес для каждого VPN-клиента, не являющегося сотрудником:

```
ccd/sysadmin1
```

```
ifconfig-push 10.8.1.1 10.8.1.2
```

```
ccd/contractor1
```

```
ifconfig-push 10.8.2.1 10.8.2.2
```

```
ccd/contractor2
```

```
ifconfig-push 10.8.2.5 10.8.2.6
```

Каждая пара адресов ifconfig-push представляет виртуальные клиентские и серверные IP-конечные точки. Они должны быть взяты из последовательных /30 подсетей, чтобы быть совместимыми с клиентами Windows и с драйвером TAP-Win32. В частности, последний октет в IP-адресе каждой пары конечных точек должен быть взят из этого набора:

```
[ 1, 2] [ 5, 6] [ 9, 10] [ 13, 14] [ 17, 18]
[ 21, 22] [ 25, 26] [ 29, 30] [ 33, 34] [ 37, 38]
[ 41, 42] [ 45, 46] [ 49, 50] [ 53, 54] [ 57, 58]
[ 61, 62] [ 65, 66] [ 69, 70] [ 73, 74] [ 77, 78]
[ 81, 82] [ 85, 86] [ 89, 90] [ 93, 94] [ 97, 98]
[101,102] [105,106] [109,110] [113,114] [117,118]
[121,122] [125,126] [129,130] [133,134] [137,138]
[141,142] [145,146] [149,150] [153,154] [157,158]
[161,162] [165,166] [169,170] [173,174] [177,178]
[181,182] [185,186] [189,190] [193,194] [197,198]
[201,202] [205,206] [209,210] [213,214] [217,218]
[221,222] [225,226] [229,230] [233,234] [237,238]
[241,242] [245,246] [249,250] [253,254]
```

Это завершает конфигурацию «OpenVPN-ГОСТ». Последний шаг — добавить брандмауэрные правила, чтобы финализировать политику доступа. Для этого примера мы воспользуемся правилами в синтаксисе iptables из Linux:

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

```

# Employee rule
iptables -A FORWARD -i tun0 -s 10.8.0.0/24 -d 10.66.4.4 -j ACCEPT

# Sysadmin rule
iptables -A FORWARD -i tun0 -s 10.8.1.0/24 -d 10.66.4.0/24 -j ACCEPT

# Contractor rule
iptables -A FORWARD -i tun0 -s 10.8.2.0/24 -d 10.66.4.12 -j ACCEPT
    
```

6.4.7 Использование альтернативных способов аутентификации

«OpenVPN-ГОСТ» имеет возможность позволять своему серверу безопасно получать логин и пароль от подключающегося клиента и использовать эту информацию как базис для аутентификации клиента.

Чтобы использовать этот способ аутентификации, сначала добавьте директиву `auth-user-pass` в клиентскую конфигурацию. Она заставит клиент «OpenVPN-ГОСТ» запрашивать у пользователя логин/пароль, передавая его на сервер по безопасному TLS-каналу.

Далее, сконфигурируйте сервер так, чтобы он использовал аутентификационный плагин, который может быть скриптом, объектом общего доступа или DLL. Сервер «OpenVPN-ГОСТ» будет вызывать этот плагин каждый раз, когда клиент VPN будет пытаться подключиться, передавая ему логин и пароль, введенные на клиенте. Аутентификационный плагин может управлять тем, позволяет ли сервер «OpenVPN-ГОСТ» клиенту соединиться, возвращая значение неудачи (1) или успеха (0).

6.4.7.1 Использование скриптовых плагинов

Скриптовые плагины можно применять, добавив директиву `auth-user-pass-verify` в серверный конфигурационный файл. Например:

```
auth-user-pass-verify auth-pam.pl via-file
```

будет применять скрипт на языке perl `auth-pam.pl` для аутентификации логина и пароля подключающихся клиентов.

Скрипт `auth-pam.pl` включен в дистрибутив «OpenVPN-ГОСТ» в подкаталоге `sample-scripts`. Он будет аутентифицировать пользователей на сервере в Linux, используя аутентификационный модуль PAM, который может в свою очередь реализовать аутентификацию методом теневого пароля, RADIUS или LDAP. `auth-pam.pl` прежде всего предназначен для демонстрационных целей. Для рабочей PAM-аутентификации используйте описанный ниже объект общего доступа `openvpn-auth-pam`.

6.4.7.2 Использование объектов общего доступа или DLL в качестве плагинов

Плагины — объекты общего доступа или DLL обычно являются скомпилированными модулями на языке C, которые загружаются сервером «OpenVPN-ГОСТ» в ходе работы. Например, если вы используете пакет «OpenVPN-ГОСТ» в Linux, основанный на RPM, то плагин `openvpn-auth-pam` уже должен быть установлен. Чтобы его использовать, добавьте строку в серверный конфигурационный файл:

```
plugin /usr/share/openvpn/plugin/lib/openvpn-auth-pam.so login
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Она прикажет серверу «OpenVPN-ГОСТ» проверять логин и пароль, введенные клиентами, с использованием PAM-модуля login.

Для реального рабочего применения лучше использовать плагин `openvpn-auth-pam`, потому что у него есть несколько преимуществ перед скриптом `auth-pam.pl`:

- Объект общего доступа `openvpn-auth-pam` для лучшей защиты использует модель выполнения с разделенными правами. Это значит, что сервер «OpenVPN-ГОСТ» может работать с уменьшенными правами с использованием директив `user nobody`, `group nobody` и `chroot`, и все равно сможет аутентифицировать клиентов с помощью файла теневого паролей, читабельного только для привилегированного пользователя.
- «OpenVPN-ГОСТ» может передавать логин и пароль в плагин через виртуальную память, а не через файл или среду, что лучше для локальной безопасности на серверной машине.
- Компилированные модули на языке C обычно работают быстрее скриптов.

Если вы хотите получить больше информации о разработке ваших собственных плагинов для использования с «OpenVPN-ГОСТ», см. файлы README в поддиректории `plugin` дистрибутива «OpenVPN-ГОСТ».

Чтобы собрать плагин `openvpn-auth-pam` на Linux, перейдите в каталог `plugin/auth-pam` в дистрибутиве «OpenVPN-ГОСТ» и запустите `make`.

6.4.7.3 Использование аутентификации по логину и паролю как единственной формы клиентской аутентификации

По умолчанию, использование `auth-user-pass-verify` или проверяющего логины и пароли плагина на сервере включит двойную аутентификацию, требуя, чтобы для аутентификации клиента были успешны и аутентификация на клиентском сертификате, и логин-парольная аутентификация.

Хотя с точки зрения безопасности это не рекомендуется, возможно отключить использование клиентских сертификатов и оставить только аутентификацию по логину и паролю. На сервере:

```
client-cert-not-required
```

Такие конфигурации обычно должны иметь строку:

```
username-as-common-name
```

Которая велит серверу использовать логин для целей индексации, как он использовал бы поле `Common Name` для клиента, аутентифицировавшегося на клиентском сертификате.

Обратите внимание, что строка `client-cert-not-required` не устраняет необходимость в серверном сертификате, так что клиент, соединяющийся с сервером, который использует `client-cert-not-required`, может удалить директивы `cert` и `key` из клиентского конфигурационного файла, но не директиву `ca`, потому что клиенту необходимо проверить серверный сертификат.

6.4.8 Добавление к конфигурации «OpenVPN-ГОСТ» двухфакторной аутентификации с использованием токенов на клиентской стороне

6.4.8.1 О двухфакторной аутентификации

Двухфакторная аутентификация — это способ аутентификации, который объединяет два элемента: что-то, что у вас есть, и что-то, что вы знаете.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Что-то, что у вас есть, должно быть устройством, которое не может быть продублировано; такое устройство может быть криптографическим токеном, содержащим закрытый ключ. Этот закрытый ключ генерируется внутри устройства и никогда его не покидает. Если пользователь, обладающий этим токеном, пытается подключиться к защищенным сервисам в удаленной сети, процесс авторизации, который дает доступ к сети или отказывает в нем, может установить, с высокой степенью уверенности, что подключающийся пользователь физически обладает известным, сертифицированным токеном.

Что-то, что вы знаете, может быть паролем (пин-кодом) для доступа к криптографическому устройству. Без предоставления корректного пароля вы не можете воспользоваться закрытым ключом. Еще одна возможность криптографических устройств — запретить использование закрытого ключа, если некорректный пароль (пин-код) был предоставлен больше, чем позволенное количество раз. Это поведение гарантирует, что если пользователь потерял свое устройство, другой человек не сможет его использовать.

Таким образом, использование токенов повышает защищенность виртуальной сети, поскольку затрудняет подключение к ней неуполномоченного пользователя.

6.4.8.2 Конфигурирование «OpenVPN-ГОСТ» для работы с токенами Rutoken

«OpenVPN-ГОСТ» может использовать закрытые ключи, записанные в файловую систему токенов Rutoken (должны быть дополнительно установлены библиотеки поддержки Rutoken).

Для использования ключей с Рутокена параметр `key` файла конфигурации «OpenVPN-ГОСТ» нужно задать следующим образом:

```
key [[ENGINE]]cryptocom:RUTOKEN:имя_контейнера
```

Имя_контейнера является числом в десятичной или шестнадцатеричной записи и должно совпадать с *именем_контейнера*, использованным при генерации ключа.

6.4.8.3 Конфигурирование «OpenVPN-ГОСТ» для работы с токенами Вьюга

«OpenVPN-ГОСТ» может использовать закрытые ключи, записанные в файловую систему токенов Вьюга (должны быть дополнительно установлены драйвера устройства). Данная возможность реализована только для 256-битных ключей.

Для использования ключей с Вьюги параметр `key` файла конфигурации «OpenVPN-ГОСТ» нужно задать следующим образом:

```
key [[ENGINE]]cryptocom:VJUGA.X
```

6.4.9 Маршрутизация всего клиентского трафика (включая веб-трафик) через VPN

6.4.10 Маршрутизация всего клиентского трафика (включая веб-трафик) через VPN

6.4.10.1 Введение

По умолчанию, когда клиент «OpenVPN-ГОСТ» активен, только сетевой трафик на сервер «OpenVPN-ГОСТ» и с него будет проходить через VPN. Общий просмотр интернет-сайтов, например, будет выполнен через прямые соединения, которые не проходят через VPN.

В некоторых случаях это поведение может быть нежелательным — вы можете захотеть, чтобы VPN-клиент туннелировал весь сетевой трафик через VPN, включая общий просмотр интернет-сайтов. Хотя этот тип конфигурации VPN заставит клиент работать медленнее, он

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

дает администратору VPN большой контроль над политиками безопасности, когда клиент одновременно соединен и с публичной сетью Интернет, и с VPN.

6.4.10.2 Реализация

Добавьте следующую директиву к серверному конфигурационному файлу:

```
push "redirect-gateway def1"
```

Если ваша VPN настроена в беспроводной сети, где все клиенты и сервер находятся в одной и той же беспроводной подсети, поставьте флаг local:

```
push "redirect-gateway local def1"
```

Передача опции redirect-gateway клиентам заставит весь IP-сетевой трафик, исходящий с клиентских машин, проходить через сервер «OpenVPN-ГОСТ». Сервер нужно будет как-то сконфигурировать, чтобы он мог работать с этим трафиком, например, соединить его с сетью Интернет через NAT или маршрутизировать через HTTP-прокси сервера.

В Linux вы можете воспользоваться вот такой командой, чтобы подключить клиентский трафик к сети Интернет через NAT:

```
iptables -t nat -A POSTROUTING -s 10.9.1.0/24 -o eth0 -j MASQUERADE
```

Эта команда предполагает, что подсеть VPN — 10.9.1.0/24 (взятая из директивы server в серверной конфигурации «OpenVPN-ГОСТ»), и что локальный интерфейс сети Ethernet — eth0.

Когда используется redirect-gateway, клиенты «OpenVPN-ГОСТ» будут маршрутизировать запросы DNS через VPN, и серверу VPN нужно будет их обрабатывать. Это может быть достигнуто передачей адреса сервера DNS подключающимся клиентам, который заместит их обычные настройки сервера DNS на время, пока VPN активна. Например:

```
push "dhcp-option DNS 10.9.1.1"
```

сконфигурирует клиенты Windows (или других операционных систем с некоторыми дополнительными скриптами) использовать 10.9.1.1 в качестве их DNS-сервера. Любой адрес, который виден с клиентов, может быть использован как адрес сервера DNS.

6.4.10.3 Предупреждения

Перенаправление всего сетевого трафика через VPN — не совсем беспроблемное предложение. Вот несколько типичных проблем, которые следует иметь в виду:

- Многие машины-клиенты «OpenVPN-ГОСТ», соединяющиеся с Интернетом, будут периодически взаимодействовать с сервером DHCP, чтобы обновить свою аренду IP-адресов. Опция redirect-gateway может не дать клиенту связаться с локальным DHCP-сервером (потому что сообщения DHCP будут маршрутизироваться через VPN), что заставит их потерять свою аренду IP-адресов.
- Существуют проблемы, связанные с передачей DNS-адресов на клиенты Windows.
- Просмотр интернет-сайтов на клиенте будет заметно медленнее.

6.4.11 Работа сервера «OpenVPN-ГОСТ» на динамическом IP-адресе

В то время как клиенты «OpenVPN-ГОСТ» могут легко достигать сервера через динамический IP-адрес без какого-либо специального конфигурирования, возникают определенные

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

проблемы, когда сам сервер имеет динамический адрес. Хотя «OpenVPN-ГОСТ» без проблем справляется с ситуацией на динамическом сервере, необходимо некоторое дополнительное конфигурирование.

Первый шаг — получить динамический DNS-адрес, который может быть сконфигурирован так, чтобы «следовать» за сервером каждый раз, как меняется IP-адрес сервера. Существуют несколько доступных провайдеров динамических DNS-услуг, например, dyndns.org.

Следующий шаг — настроить механизм, чтобы каждый раз, когда IP-адрес сервера меняется, имя динамического DNS быстро получало бы новый IP-адрес, позволяя клиентам найти сервер по его новому IP-адресу. Есть два основных способа это сделать:

- Использовать оборудование маршрутизатора NAT с поддержкой динамического DNS (например, Linksys BEFSR41). Большинство недорогих и широкодоступных маршрутизаторов NAT обладают возможностью обновлять динамическое имя DNS каждый раз, как новая аренда DHCP получена с ISP. Эта настройка идеальна, когда сервер «OpenVPN-ГОСТ» является компьютером с одним сетевым адаптером внутри брандмауэра.
- Использовать динамическое приложение DNS-клиента, например, ddclient (<http://sourceforge.net/apps/trac/ddclient>) для обновления динамического DNS-адреса, как только поменяется IP-адрес сервера. Эта настройка идеальна, когда машина, на которой работает «OpenVPN-ГОСТ», имеет несколько сетевых адаптеров и работает как брандмауэр/гейт. Чтобы реализовать эту настройку, вам необходимо настроить скрипт, который будет выполняться вашим программным приложением DHCP-клиента каждый раз, как происходит смена IP-адреса. Этот скрипт должен а) выполнять ddclient, чтобы уведомить ваш провайдер динамического DNS о вашем новом IP-адресе и б) перезапустить серверный демон «OpenVPN-ГОСТ».

Клиент «OpenVPN-ГОСТ» по умолчанию почувствует, когда сменится IP-адрес сервера, если клиентская конфигурация использует директиву `remote`, которая соотносится с именем динамического DNS. Обычная цепь событий такова: а) клиенту «OpenVPN-ГОСТ» не удастся получить своевременные поддерживающие сообщения со старого IP-адреса сервера, что запускает перезагрузку, и б) перезагрузка заставляет пересмотреть имя DNS в директиве `remote`, позволяя клиенту переподключиться к серверу по его новому IP-адресу.

6.4.12 Подключение к серверу «OpenVPN-ГОСТ» через HTTP-прокси

«OpenVPN-ГОСТ» поддерживает соединения через HTTP-прокси, со следующими моделями аутентификации:

- Нет аутентификации на прокси
- Basic аутентификация на прокси
- NTLM аутентификация на прокси

Добавьте директиву `http-proxy` в клиентский конфигурационный файл.

Например, предположим, что у вас HTTP-прокси сервер на клиентской локальной сети на 192.168.4.1, который слушает соединения на порту 1080. Добавьте следующую строку к клиентской конфигурации:

```
http-proxy 192.168.4.1 1080
```

Предположим, что HTTP-прокси требует аутентификации Basic:

```
http-proxy 192.168.4.1 1080 stdin basic
```

Предположим, что HTTP-прокси требует аутентификации NTLM:

```
http-proxy 192.168.4.1 1080 stdin ntlm
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Два вышеприведенных аутентификационных примера заставят «OpenVPN-ГОСТ» запросить логин и пароль со стандартного ввода. Если вы вместо этого предпочитаете поместить логин и пароль в файл, замените stdin именем файла и поместите логин в первую строку этого файла, а пароль во вторую.

6.4.13 Соединение с совместно используемым ресурсом Samba через «OpenVPN-ГОСТ»

Этот пример предназначен для того, чтобы показать, как клиенты «OpenVPN-ГОСТ» могут соединяться с совместно используемым ресурсом Samba через маршрутизированный туннель dev tun. Если вы используете «OpenVPN-ГОСТ» типа «мост» (dev tap), вам, вероятно, не нужно следовать этим инструкциям, поскольку клиенты «OpenVPN-ГОСТ» должны видеть машины серверной стороны в своем сетевом окружении.

Для этого примера предположим, что:

- Серверная локальная сеть использует подсеть 10.66.0.0/24,
- Диапазон IP-адресов VPN использует 10.8.0.0/24 (как указано в директиве server в серверном конфигурационном файле «OpenVPN-ГОСТ» .)
- Сервер Samba имеет IP-адрес 10.66.0.4 и
- Сервер Samba уже был сконфигурирован и доступен из местной локальной сети.

Если серверы Samba и «OpenVPN-ГОСТ» работают на различных машинах, удостоверьтесь, что вы выполнили указания раздела «Расширение области действия VPN с включением дополнительных машин в клиентскую или серверную подсеть».

Далее отредактируйте конфигурационный файл сервера Samba (smb.conf). Удостоверьтесь, что директива hosts allow позволит клиентам «OpenVPN-ГОСТ», приходящим из подсети 10.9.1.0/24, устанавливать соединение. Например:

```
hosts allow = 10.66.0.0/24 10.9.1.0/24 127.0.0.1
```

Если серверы Samba и «OpenVPN-ГОСТ» работают на одной и той же машине, вы, возможно, захотите отредактировать директиву interfaces в файле smb.conf так, чтобы также слушать на подсети 10.9.1.0/24 интерфейса TUN:

```
interfaces = 10.66.0.0/24 10.9.1.0/24
```

Если серверы Samba и «OpenVPN-ГОСТ» работают на одной и той же машине, подключитесь с клиента «OpenVPN-ГОСТ» к совместно используемому ресурсу Samba с использованием имени каталога:

```
\\10.9.1.1\\sharename
```

Если серверы Samba и «OpenVPN-ГОСТ» работают на разных машинах, используйте имя каталога:

```
\\10.66.0.4\\sharename
```

Например, из окна командной строки:

```
net use z: \\10.66.0.4\\sharename /USER:myusername
```

6.4.14 Реализация конфигурации балансировки нагрузки/восстановления после сбоя

6.4.14.1 Клиент

Клиентская конфигурация «OpenVPN-ГОСТ» может указывать на несколько серверов для балансировки нагрузки и восстановления после отказа. Например:

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

```
remote server1.mydomain
remote server2.mydomain
remote server3.mydomain
```

прикажет клиенту «OpenVPN-ГОСТ» пытаться устанавливать соединение с server1, server2 и server3 в этом порядке. Если существующее соединение разорвано, клиент OpenVPN попытается восстановить соединение с последним сервером, с которым соединение было установлено, а если это не удастся, перейдет на следующий сервер в списке. Вы также можете указать клиенту «OpenVPN-ГОСТ» рандомизовать свой список серверов при загрузке, чтобы клиентская нагрузка была вероятностно распределена по диапазону серверов.

```
remote-random
```

Если вы также хотите, чтобы неудачи разрешения DNS заставляли клиент «OpenVPN-ГОСТ» переходить на следующий сервер в списке, добавьте следующее:

```
resolv-retry 60
```

Параметр 60 велит клиенту «OpenVPN-ГОСТ» пытаться разрешить каждое удаленное имя DNS в течение 60 секунд, прежде чем переходить на следующий сервер в списке.

Список серверов может также указывать на несколько серверных демонов «OpenVPN-ГОСТ», работающих на одной и той же машине, каждый из которых слушает соединения на собственном порту, например:

```
remote smp-server1.mydomain 8000
remote smp-server1.mydomain 8001
remote smp-server2.mydomain 8000
remote smp-server2.mydomain 8001
```

6.4.14.2 Список серверов

Если ваши сервера — многопроцессорные машины, запуск нескольких демонов «OpenVPN-ГОСТ» на каждом сервере может иметь преимущества с точки зрения скорости выполнения.

«OpenVPN-ГОСТ» также поддерживает директиву remote, указывающую на имя DNS, которое обладает несколькими записями А в зонной конфигурации для домена. В этом случае клиент «OpenVPN-ГОСТ» будет случайным образом выбирать одну из записей А каждый раз, как домен разрешается.

6.4.14.3 Сервер

Самый простой подход к конфигурации балансировки нагрузки и восстановления после отказа на сервере — использовать эквивалентные конфигурационные файлы на каждом сервере в кластере, за исключением использования различных диапазонов виртуальных IP-адресов для каждого сервера. Например:

```
server1
server 10.8.0.0 255.255.255.0
server2
server 10.8.1.0 255.255.255.0
server3
server 10.8.2.0 255.255.255.0
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6.4.15 Конфигурирование «OpenVPN-ГОСТ» для автоматического запуска при старте системы

Недостаток стандартов в этой области означает, что большинство операционных систем имеет собственный способ конфигурирования демонов/сервисов для запуска при запуске системы. Лучший способ получить эту функциональность сконфигурированной по умолчанию — установить «OpenVPN-ГОСТ» как пакет, например, через RPM на Linux или воспользовавшись инсталлятором Windows.

6.4.15.1 Linux

Если вы устанавливаете «OpenVPN-ГОСТ» через пакет RPM на Linux, инсталлятор установит initscript. При выполнении initscript будет искать конфигурационные файлы .conf в /etc/openvpn, и если таковые найдены, запустит отдельный демон «OpenVPN-ГОСТ» для каждого файла.

6.4.15.2 Windows

Инсталлятор Windows установит сервисную оболочку, но оставит ее отключенной по умолчанию. Чтобы активировать ее, идите в Control Panel / Administrative Tools / Services, выберите сервис OpenVPN, щелкните правой клавишей на свойствах и установите Startup Type в Automatic. Это сконфигурирует сервис для автоматического старта при следующей перезагрузке.

При запуске сервисная оболочка «OpenVPN-ГОСТ» просканирует каталог \Program Files\OpenVPN\config в поисках конфигурационных файлов .ovpn, начиная отдельный процесс «OpenVPN-ГОСТ» для каждого файла.

6.4.16 Запуск VPN и тест на начальную подключаемость

6.4.16.1 Запуск сервера

Сначала убедитесь, что сервер «OpenVPN-ГОСТ» будет доступен из интернета. Это значит:

- Открыть TCP-порт 1194 на брандмауэре (или любой другой TCP-порт, который вы сконфигурировали) или
- Установить правило форвардинга порта, чтобы произвести форвардинг TCP-порта 1194 с брандмауэра/гейта на машину, где работает сервер «OpenVPN-ГОСТ» .

Далее, убедитесь, что интерфейс TUN/TAP не за брандмауэром.

Чтобы упростить поиск ошибок, лучше сначала запустить сервер «OpenVPN-ГОСТ» из командной строки (или щелкнуть правой клавишей по файлу .ovpn в Windows), а не запускать ее как демон или сервис:

```
openvpn [server config file]
```

Нормальное начало работы сервера должно выглядеть примерно так (вывод может быть разным на разных операционных системах):

```
Mon Jan 16 15:19:08 2017 OpenVPN 2.3.13 i686-pc-linux-gnu [SSL (OpenSSL)]
[EPOLL] [MH] [IPv6] built on Jan 16 2017
Mon Jan 16 15:19:08 2017 library versions: CryptoPack 3.0 OpenSSL 1.0.2j
Mon Jan 16 15:19:08 2017 Initializing OpenSSL support for engine 'gost'
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

```

Mon Jan 16 15:19:08 2017 WARNING: file 'server.key' is group
or others accessible
Mon Jan 16 15:19:08 2017 TUN/TAP device tap0 opened
Mon Jan 16 15:19:08 2017 do_ifconfig, tt->ipv6=0,
tt->did_ifconfig_ipv6_setup=0
Mon Jan 16 15:19:08 2017 /sbin/ifconfig tap0 10.9.1.1
netmask 255.255.255.0 mtu 1500 broadcast 10.9.1.255
Mon Jan 16 15:19:08 2017 Listening for incoming TCP connection on [undef]
Mon Jan 16 15:19:08 2017 TCPv4_SERVER link local (bound): [undef]
Mon Jan 16 15:19:08 2017 TCPv4_SERVER link remote: [undef]
Mon Jan 16 15:19:08 2017 Initialization Sequence Completed
Mon Jan 16 15:19:12 2017 /sbin/ifconfig tap0 0.0.0.0
Mon Jan 16 15:19:12 2017 SIGINT[hard,] received, process exiting
    
```

6.4.16.2 Запуск клиента

Как и в случае серверной конфигурации, лучше запустить клиент «OpenVPN-ГОСТ» из командной строки (или в Windows щелкнуть правой клавишей мыши по файлу client.ovpn), а не запускать ее как демон или сервис:

```
openvpn [client config file]
```

Нормальное начало работы клиента на Windows будет похоже на серверный вывод, приведенный выше, и должен закончиться сообщением Initialization Sequence Completed.

Теперь попробуйте отправить сигнал ping через VPN от клиента. Если вы используете маршрутизацию (т.е. dev tun в серверном конфигурационном файле), попробуйте:

```
ping 10.9.1.0
```

Если вы используете VPN типа «мост» (т.е. dev tap в серверном конфигурационном файле), попытайтесь отправить сигнал ping на IP-адрес машины на подсети серверной сети Ethernet.

Если сигнал проходит успешно, поздравляем! У вас теперь действующая VPN.

6.4.16.3 Поиск ошибок

Если сигнал ping не прошел или инициализация клиента «OpenVPN-ГОСТ» не закончилась, вот список обычных симптомов и их решений:

1. Вы получаете сигнал ошибки: TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity). Эта ошибка указывает, что клиент не сумел установить сетевую связь с сервером.

Решения:

- Убедитесь, что клиент использует корректный hostname/IP-адрес и номер порта, который позволит ему соединиться с сервером «OpenVPN-ГОСТ» .
- Если машина сервера «OpenVPN-ГОСТ» является компьютером с одним сетевым адаптером внутри защищенной LAN, убедитесь, что вы пользуетесь корректным правилом форвардинга порта на брандмауэр сервера. Например, предположим, что ваш сервер «OpenVPN-ГОСТ» находится на 192.168.4.4 внутри брандмауэра, слушающая клиентские подключения на TCP-порту 1194. Гейт NAT, обслуживающий подсеть 192.168.4.x должен иметь правило форвардинга порта, которое говорит «переадресовать TCP-порт 1194 с моего публичного IP-адреса на 192.168.4.4.»

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

- Откройте брандмауэр сервера, чтобы разрешить входящие соединения на TCP-порт 1194 (или любой TCP-порт, который вы сконфигурировали в серверном конфигурационном файле).
2. Вы получаете сообщение об ошибке: Initialization Sequence Completed with errors — Эта ошибка может произойти на Windows, если а) у вас нет запущенного доступного сервиса DHCP или б) вы используете определенные персональные брандмауэры третьей стороны на XP SP2.
Решение: запустите сервер для клиента DHCP и убедитесь, что вы используете персональный брандмауэр, который, как точно известно, корректно работает на XP SP2.
 3. Вы получаете сообщение Initialization Sequence Completed, но сигнал ping не проходит — это обычно указывает, что брандмауэр на серверной или клиентской стороне блокирует передачу по сети VPN, фильтруя на интерфейсе TUN/TAP.
Решение: отключите в клиентском брандмауэре (если он существует) фильтрацию интерфейса TUN/TAP на клиенте. Например, на Windows XP SP2 вы можете это сделать, пойдя на Windows Security Center -> Windows Firewall -> Advanced и сняв галочку, которая соответствует адаптеру TAP-Win32 (отключение в клиентском брандмауэре фильтрации адаптера TUN/TAP в общем рационально с точки зрения безопасности, поскольку вы в сущности говорите брандмауэру не блокировать аутентифицированную передачу VPN). Также убедитесь, что интерфейс TUN/TAP на сервере не фильтруется брандмауэром (заметьте, что избирательное перекрытие брандмауэром интерфейса TUN/TAP на серверной стороне может иметь определенные выгоды с точки зрения безопасности.)

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7 Использование

7.1 Запуск на ОС семейства Windows

После того, как вы выполните установку, «OpenVPN-ГОСТ» готова к использованию и ассоциирована с файлами с расширением .ovpn.

Чтобы запустить «OpenVPN-ГОСТ», вы можете:

- Щелкнуть правой клавишей на конфигурационном файле «OpenVPN-ГОСТ» (.ovpn) и выбрать Start OpenVPN с этим конфигурационным файлом. Чтобы выйти, можно воспользоваться клавишей F4.
- Запустить «OpenVPN-ГОСТ» из командной строки Windows такой командой, как:

```
openvpn [config file]
```

Запущенную из окна командной строки «OpenVPN-ГОСТ» можно отключить клавишей F4.

- Запустить «OpenVPN-ГОСТ» как сервис, поместив один или больше конфигурационных файлов .ovpn в каталог \Program Files\OpenVPN\config и запустив сервис «OpenVPN-ГОСТ», который может управляться из Start Menu -> Control Panel -> Administrative Tools -> Services.

7.2 Запуск на ОС, не входящих в семейство Windows

После установки и настройки «OpenVPN-ГОСТ» готова к использованию. Если «OpenVPN-ГОСТ» не была сконфигурирована для автозапуска при старте системы, можно запустить «OpenVPN-ГОСТ» из командной строки:

```
openvpn [config file]
```

7.3 Управление запущенным процессом «OpenVPN-ГОСТ»

7.3.1 Работа на Linux/BSD/Unix

«OpenVPN-ГОСТ» принимает несколько сигналов:

SIGUSR1 — условный перезапуск, предназначенный для перезапуска без привилегий суперпользователя

SIGHUP — жесткий перезапуск

SIGUSR2 — статистика исходящего соединения в файл журнала или системный журнал

SIGTERM, SIGINT — выход

Используйте директиву writpid, чтобы записать PID демона «OpenVPN-ГОСТ» в файл, чтобы вы знали, куда отправить сигнал (если вы запускаете openvpn с помощью initscript, скрипт может уже передавать директиву -writpid в командную строку openvpn).

7.3.2 Работа в Windows в графическом интерфейсе

Хотя «OpenVPN-ГОСТ» может быть запущена как демон, сервис или из командной строки, возможно управлять «OpenVPN-ГОСТ» через графический интерфейс.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.3 Работа в окне командной строки Windows

В Windows вы можете запустить «OpenVPN-ГОСТ», кликнув правой клавишей мыши на конфигурационном файле «OpenVPN-ГОСТ» (файл .ovpn) и выбрав Start OpenVPN on this config file.

Если «OpenVPN-ГОСТ» запущена таким образом, доступны несколько клавишных команд:

- F1 — условный перезапуск (не закрывает/переоткрывает адаптер TAP)
- F2 — показать статистику соединения
- F3 — жесткий перезапуск
- F4 — выход

7.3.4 Работа в качестве сервиса Windows

Когда «OpenVPN-ГОСТ» запущена в качестве сервиса на Windows, управлять ей можно только:

- Через менеджер управления сервисами (Control Panel / Administrative Tools / Services), который дает возможность запускать и выключать сервис;
- Через интерфейс управления (см. раздел 7.3.7)

7.3.5 Модификация конфигурации запущенного сервера

Хотя большинство изменений конфигурации требуют перезапуска сервера, есть две директивы, связанные с файлами, которые могут быть динамически изменены в ходе работы, и которые немедленно повлияют на сервер без необходимости перезапускать процесс.

`client-config-dir` — эта директива устанавливает каталог клиентской конфигурации, которую «OpenVPN-ГОСТ» будет сканировать при каждом входящем соединении в поисках клиент-специфичного конфигурационного файла. Файлы в этом каталоге могут быть изменены в ходе работы, без перезапуска сервера. Обратите внимание, что изменения в этом каталоге повлияют только на новые соединения, не на существующие соединения. Если вы хотите, чтобы изменение клиент-специфичного конфигурационного файла немедленно подействовало на уже соединившегося клиента (или на клиента, который уже отключился, но сервер еще не уничтожил его экземпляр), уничтожьте экземпляр клиента, воспользовавшись интерфейсом управления (см. раздел 7.3.7). Это заставит клиента переподключиться и использовать новый файл `client-config-dir`.

`ctrl-verify` — эта директива именуется список отзыва сертификатов, описанный ниже в разделе «Отзыв сертификатов». Файл списка отзыва сертификатов можно менять в ходе работы, и изменения немедленно повлияют на новые соединения, или на существующие соединения, которые обновляют свой канал SSL/TLS (по умолчанию это происходит раз в час). Если вы хотите уничтожить подключенного клиента, чей сертификат только что добавили в список отзыва сертификатов, воспользуйтесь интерфейсом управления (см. раздел 7.3.7).

7.3.6 Файл статуса

Умолчательный файл `server.conf` имеет строку `status openvpn-status.log`

которая будет выводить список текущих клиентских соединений в файл `openvpn-status.log` раз в минуту.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.7 Использование интерфейса управления

Интерфейс управления «OpenVPN-ГОСТ» позволяет административно управлять «OpenVPN-ГОСТ» из внешней программы через TCP-сокеты.

Интерфейс был специально разработан для разработчиков графического интерфейса и для тех, кто хотел бы программно или удаленно управлять демоном «OpenVPN-ГОСТ».

Интерфейс управления реализован с использованием клиент-серверного TCP-соединения, где «OpenVPN-ГОСТ» будет слушать на предоставленном IP-адресе и порту входящие управляющие клиентские соединения.

Протокол управления сейчас текстовый без сложного защитного слоя. По этой причине рекомендуется, чтобы интерфейс управления слушал или на localhost (127.0.0.1) или на локальном адресе VPN. Возможно удаленное соединение с интерфейсом управления поверх самой VPN, хотя некоторые возможности в этом режиме будут ограничены, такие, как способность предоставлять пароли от закрытых ключей.

Интерфейс управления включается в конфигурационном файле «OpenVPN-ГОСТ» с помощью следующих директив:

- management
- management-query-passwords
- management-log-cache

Когда «OpenVPN-ГОСТ» запущена с подключенным слоем управления, вы можете подключиться через telnet к порту управления (обязательно используйте клиент telnet, который понимает «грубый» режим).

Подключившись к порту управления, вы можете использовать команду help для вывода списка всех команд.

7.3.7.1 Команда echo

Эта команда используется, чтобы дать возможность или вписать в конфигурационный файл «OpenVPN-ГОСТ», или передать на клиент «OpenVPN-ГОСТ» с сервера параметры, специфичные для графического интерфейса.

Примеры команды:

echo on — включает нотификацию сообщений echo в реальном времени

echo all — выводит текущий список истории echo

echo off — отключает нотификацию сообщений echo в реальном времени

echo on all — атомно включает нотификацию в реальном времени, плюс показывает все сообщения в буфере истории

Например, предположим, что вы разрабатываете графический интерфейс «OpenVPN-ГОСТ» и хотите дать серверу «OpenVPN-ГОСТ» способность просить интерфейс забыть все сохраненные пароли.

В серверном конфигурационном файле «OpenVPN-ГОСТ» добавьте:

push "echo forget-passwords"

Когда клиент «OpenVPN-ГОСТ» получает свой список директив с сервера, директива echo forget-passwords будет в списке и заставит интерфейс управления сохранить строку forget-passwords в своем списке параметров echo.

Клиент управления может использовать echo all для вывода полного списка параметров echo, echo on для включения нотификации этих параметров в реальном времени через префикс >ECHO:, или echo off для отключения нотификации в реальном времени.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Когда графический интерфейс подключается к сокету управления «OpenVPN-ГОСТ», он может отдать команду `echo all`, которая даст вывод типа:

```
1101519562, forget-passwords
END
```

По сути команда `echo` позволила нам передать параметры с сервера «OpenVPN-ГОСТ» на клиент, а затем на клиент управления (такой как графический интерфейс). Большое целое число — юниксовая дата/время, когда был получен параметр `echo`.

Если клиент управления отдал команду `echo on`, она включит нотификацию параметров `echo` в реальном времени. В этом случае наше сообщение `forget-passwords` будет иметь вывод типа:

```
>ECHO:1101519562, forget-passwords
```

Как и команда `log`, команда `echo` может атомно показывать историю, одновременно активируя обновления в реальном времени:

```
echo on all
```

Размер буфера `echo` в настоящее время жестко ограничен 100 сообщениями.

7.3.7.2 Команда `exit`, `quit`

Закрывает сеанс управления и восстанавливает слушание соединений от других клиентов на порту управления. В настоящее время демон «OpenVPN-ГОСТ» может поддерживать самое большее один клиент управления в любой момент времени.

7.3.7.3 Команда `help`

Выводит краткий список команд.

7.3.7.4 Команда `hold`

Команда `hold` может быть использована для манипуляций с флагом `hold` или освобождения «OpenVPN-ГОСТ» из состояния `hold`.

Если флаг `hold` установлен при первоначальном запуске или перезагрузке, «OpenVPN-ГОСТ» будет находиться в замершем состоянии перед инициализацией туннеля, пока интерфейс управления не получит команду `hold release`.

Директива «OpenVPN-ГОСТ» `-management-hold` может быть использована, чтобы запустить «OpenVPN-ГОСТ» с установленным флагом `hold`.

Установка флага `hold` постоянна и не будет переключена перезагрузками.

«OpenVPN-ГОСТ» укажет, что она в состоянии `hold`, отправив нотификацию в реальном времени клиенту управления:

```
>HOLD:Waiting for hold release
```

Примеры команды:

`hold` — показать текущий флаг `hold`, 0=отключен, 1=включен.

`hold on` — включить флаг `hold`, чтобы будущие перезагрузки приводили в состояние `hold`.

`hold off` — отключить флаг `hold`, чтобы будущие перезагрузки не приводили в состояние `hold`.

`hold release` — выйти из состояния `hold` и запустить «OpenVPN-ГОСТ», но не изменить текущее состояние флага `hold`.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.7.5 Команда kill

В режиме сервера уничтожить конкретный экземпляр клиента.

Примеры команды:

kill Test-Client — уничтожить экземпляр клиента с Common Name «Test-Client».

kill 1.2.3.4.4000 — уничтожить экземпляр клиента с исходящим адресом и портом 1.2.3.4.4000.

Используйте команду «status», чтобы посмотреть, какие клиенты подключены.

7.3.7.6 Команда log

Показывает файл журнала «OpenVPN-ГОСТ» . Интерфейсом управления кэшируются только последние *n* строк файла журнала, где *n* управляется «OpenVPN-ГОСТ» — директивой management-log-cache.

Примеры команды:

log on — Включить вывод журнальных сообщений в реальном времени

log all — Показать текущую кэшированную историю файла журнала

log on all — Атомно показать всю текущую кэшированную историю файла журнала, потом включить вывод журнальных сообщений в реальном времени

log off — Отключить нотификацию сообщений журнала в реальном времени

log 20 — показать последние 20 строк истории файла журнала

Формат нотификации в реальном времени:

Сообщения журнала в реальном времени начинаются с префикса >LOG:, за которым следуют разделенные запятой поля:

1. юниксовое целое дата/время
2. ноль или больше флагов сообщений в одной строке:
 - I — информационное
 - F — фатальная ошибка
 - N — не фатальная ошибка
 - W — предупреждение
 - D — отладка, и
3. текст сообщения.

7.3.7.7 Команда mute

Меняет параметр «OpenVPN-ГОСТ» –mute. Этот параметр используется, чтобы не выводить повторяющиеся сообщения одной и той же категории сообщений.

Примеры команды:

mute 40 — установить параметр mute в 40

mute — показать текущее значение mute

7.3.7.8 Команда net

(Только для Windows) Дает эквивалент вывода директивы «OpenVPN-ГОСТ» –show-net. Вывод включает взгляд «OpenVPN-ГОСТ» на список системных сетевых адаптеров и таблицу маршрутизации, основанный на информации, возвращенной Windows IP helper API.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.7.9 Команда password и username

Команда password используется, чтобы передавать пароли в «OpenVPN-ГОСТ» .

Если «OpenVPN-ГОСТ» запущена с директивой `–management-query-passwords`, она будет запрашивать у интерфейса управления пароли закрытых ключей и пароль/логин `–auth-user-pass`.

Когда «OpenVPN-ГОСТ» нуждается в пароле с интерфейса управления, она выводит сообщение `>PASSWORD:` в реальном времени.

Пример 1:

```
>PASSWORD:Need 'Private Key' password
```

«OpenVPN-ГОСТ» указывает, что она нуждается в пароле типа «закрытый ключ».

Клиент управления должен отвечать на этот запрос так:

```
password "Private Key" foo
```

Пример 2:

```
>PASSWORD:Need 'Auth' username/password
```

«OpenVPN-ГОСТ» нуждается в пароле `–auth-user-pass`. Клиент управления должен ответить:

```
username "Auth" foo
```

```
password "Auth" bar
```

Сами логин и пароль могут быть в кавычках, и специальные символы, такие как двойные кавычки или обратный слэш, должны быть под escape-последовательностью, например:

```
password "Private Key" "foo\"bar"
```

Правила составления escape-последовательностей такие же, как для конфигурационного файла.

Тип сообщений `PASSWORD` в реальном времени может также использоваться, чтобы указать некорректность пароля или невыполнение других видов аутентификации:

Пример 3: пароль закрытого ключа некорректен и «OpenVPN-ГОСТ» завершает работу:

```
>PASSWORD:Verification Failed: 'Private Key'
```

Пример 4: логин/пароль `–auth-user-pass` некорректен, и «OpenVPN-ГОСТ» завершает работу:

```
>PASSWORD:Verification Failed: 'Auth'
```

7.3.7.10 Команда signal

Команда signal посылает сигнал демону «OpenVPN-ГОСТ» . Сигнал может быть одним из `SIGHUP`, `SIGTERM`, `SIGUSR1` или `SIGUSR2`.

Пример команды:

```
signal SIGUSR1 — посылает демону сигнал SIGUSR1
```

7.3.7.11 Команда state

Показывает текущее состояние «OpenVPN-ГОСТ» , показывает историю состояний или включает нотификацию перемен состояния в реальном времени.

Существуют состояния «OpenVPN-ГОСТ» :

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

- CONNECTING — исходное состояние «OpenVPN-ГОСТ»
- WAIT — (только клиент) ждет первого ответа от сервера
- AUTH — (только клиент) аутентифицируется на сервере
- GET_CONFIG — (только клиент) загружает конфигурационные опции с сервера.
- ASSIGN_IP — присваивает IP-адрес виртуальному сетевому интерфейсу.
- ADD_ROUTES — добавляет к системе маршрутизацию
- CONNECTED — инициализационная последовательность завершена.
- RECONNECTING — произошла перезагрузка
- EXITING — в процессе аккуратного выхода.

Примеры команды:

state — Вывести текущее состояние «OpenVPN-ГОСТ» .

state on — включить нотификацию изменений состояния в реальном времени

state off — выключить нотификацию изменений состояния в реальном времени

state all — вывести текущую историю состояния

state 3 — вывести 3 последних перехода состояний

state on all — атомно показать историю состояний и в то же время включить нотификацию будущих переходов состояний в реальном времени.

Формат вывода состоит из 4 разделенных запятыми параметров:

1. целое юниксовое дата/время
2. наименование состояния
3. опциональная описательная строка (используется в основном при RECONNECTING или EXITING, чтобы показать причину разрыва связи)
4. опциональный локальный IP-адрес TUN/TAP (показывается для ASSIGN_IP и CONNECTED).

Сообщения о состояниях в реальном времени будут иметь префикс >STATE:.

7.3.7.12 Команда status

Показывает текущую информацию о статусе демона, в том же формате, какой используется директивой «OpenVPN-ГОСТ» –status.

Примеры команды:

status — показать информацию о статусе, используя умолчательную версию формата статуса.

status 2 — показать информацию о статусе, используя версию формата статуса 2.

7.3.7.13 Команда username

См. раздел 7.3.7.9.

7.3.7.14 Команда verb

Изменяет параметр «OpenVPN-ГОСТ» –verb. Параметр verb контролирует подробность вывода и может варьироваться от 0 (нет вывода) до 15 (максимальный вывод).

Примеры команды:

verb 4 — изменяет параметр verb в 4

verb — показать текущую установку параметра verb

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.7.15 Команда version

Показывает текущие версии «OpenVPN-ГОСТ» и интерфейса управления.

7.3.7.16 Команда auth-retry

Устанавливает параметр auth-retry, контролирующий, как «OpenVPN-ГОСТ» отвечает на аутентификационные ошибки логина/пароля.

Примеры команды:

auth-retry interact — не завершать работу, если введены некорректные логин и пароль. Запросить новый ввод и повторить попытку.

7.3.7.17 Формат сообщений в реальном времени

Интерфейс управления «OpenVPN-ГОСТ» производит два вида вывода:

1. ответ на команду
2. асинхронный вывод в реальном времени, который может быть сгенерирован в любое время.

Сообщения в реальном времени начинаются с символа > в первой колонке, за которым немедленно следует ключевое слово, указывающее тип сообщения. Сейчас определены следующие типы:

ECHO — сообщения echo, подобные контролируемым командой echo

FATAL — фатальная ошибка, сообщение выводится в журнал сразу перед завершением работы «OpenVPN-ГОСТ» .

HOLD — используется для указания, что «OpenVPN-ГОСТ» находится в замершем состоянии и не начнет работать, пока не получит команду hold release.

INFO — информационные сообщения, такие, как приветственное сообщение.

LOG — вывод журнального сообщения, подобный контролируемым командой log

PASSWORD — используется, чтобы сообщить клиенту управления, что «OpenVPN-ГОСТ» нуждается в пароле, а также чтобы сообщить о неудаче проверки пароля.

STATE — показывает текущее состояние «OpenVPN-ГОСТ» , подобное контролируемому командой state.

7.3.7.18 Разбор команд

«OpenVPN-ГОСТ» использует тот же лексический анализатор командных строк, что используется парсером конфигурационного файла «OpenVPN-ГОСТ» .

Параметры разделяются пробелом.

Двойные кавычки ("") можно использовать, чтобы ограничить параметры, содержащие пробел

Используются escape-последовательности, основанные на обратном слэше, со следующей символикой:

\\ — означает один символ обратного слэша (\) \ " — передает буквальный символ двойных кавычек (") , не интерпретируя его как ограничение параметра \[SPACE] — передает буквальный символ пробела или табуляции, не интерпретируя его как разделитель параметров.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.3.8 Управление процессом «OpenVPN-ГОСТ» с помощью интерфейса управления

Интерфейс управления «OpenVPN-ГОСТ» дает большие возможности управления процессом «OpenVPN-ГОСТ». Вы можете использовать интерфейс управления непосредственно, подключаясь через telnet к порту интерфейса управления, или косвенно, используя графический интерфейс «OpenVPN-ГОСТ», который сам подключается к интерфейсу управления.

Чтобы включить интерфейс управления на сервере или клиенте «OpenVPN-ГОСТ», добавьте к конфигурационному файлу следующую строку:

```
management localhost 7505
```

Эта строка прикажет «OpenVPN-ГОСТ» слушать на TCP-порту 7505 клиенты интерфейса управления (порт 7505 — произвольный выбор, вы можете выбрать любой свободный порт)

Когда «OpenVPN-ГОСТ» запущена, вы можете подключиться к интерфейсу управления, воспользовавшись клиентом telnet. Например:

```
ai:~ # telnet localhost 7505
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
>INFO:OpenVPN Management Interface Version 1 -- type 'help' for more info
help
Management Interface for OpenVPN 2.3.13 i686-pc-linux-gnu [SSL (OpenSSL)]
[EPOLL] [MH] [IPv6] built on Jan 16 2017
Commands:
auth-retry t           : Auth failure retry mode (none,interact,nointeract).
bytecount n           : Show bytes in/out, update every n secs (0=off).
echo [on|off] [N|all] : Like log, but only show messages in echo buffer.
exit|quit             : Close management session.
forget-passwords      : Forget passwords entered so far.
help                  : Print this message.
hold [on|off|release] : Set/show hold flag to on/off state, or
                       release current hold and start tunnel.
kill cn               : Kill the client instance(s) having common name cn.
kill IP:port          : Kill the client instance connecting from IP:port.
load-stats            : Show global server load stats.
log [on|off] [N|all]  : Turn on/off realtime log display
                       + show last N lines or 'all' for entire history.
mute [n]              : Set log mute level to n, or show level
                       if n is absent.
needok type action    : Enter confirmation for NEED-OK request of 'type',
                       where action = 'ok' or 'cancel'.
needstr type action   : Enter confirmation for NEED-STR request of 'type',
                       where action is reply string.
net                   : (Windows only) Show network info and routing table.
password type p       : Enter password p for a queried OpenVPN password.
remote type [host port] : Override remote directive, type=ACCEPT|MOD|SKIP.
proxy type [host port flags] : Enter dynamic proxy server info.
pid                   : Show process ID of the current OpenVPN process.
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

```

client-auth CID KID      : Authenticate client-id/key-id CID/KID (MULTILINE)
client-auth-nt CID KID  : Authenticate client-id/key-id CID/KID
client-deny CID KID R [CR] : Deny auth client-id/key-id CID/KID with
                             log reason text R and optional client
                             reason text CR
client-kill CID [M]      : Kill client instance CID with message M
                             (def=RESTART)
env-filter [level]       : Set env-var filter level
client-pf CID            : Define packet filter for client CID (MULTILINE)
rsa-sig                  : Enter an RSA signature in response to >RSA_SIGN
                             challenge
                             Enter signature base64 on subsequent lines followed
signal s                  : Send signal s to daemon,
                             s = SIGHUP|SIGTERM|SIGUSR1|SIGUSR2.
state [on|off] [N|all]  : Like log, but show state history.
status [n]               : Show current daemon status info using format #n.
test n                   : Produce n lines of output for testing/debugging.
username type u          : Enter username u for a queried OpenVPN username.
verb [n]                 : Set log verbosity level to n,
                             or show if n is absent.
version                  : Show current version number.
END
exit
Connection closed by foreign host.
ai:~ #
    
```

7.4 Усиление безопасности «OpenVPN-ГОСТ»

Одна из часто повторяемых максим сетевой безопасности состоит в том, что никогда не следует целиком полагаться на один компонент защиты, потому что его отказ вызывает катастрофический провал в безопасности. «OpenVPN-ГОСТ» предоставляет несколько механизмов, предоставляющих возможность добавить дополнительные слои защиты, чтобы отгородиться от подобного исхода.

7.4.1 tls-auth

Директива `tls-auth` добавляет дополнительную подпись HMAC ко всем пакетам хэндшейка SSL/TLS для проверки целостности. Эта подпись HMAC предоставляет дополнительный слой защиты над и за тем, что предоставляется SSL/TLS. Она может защитить от:

- DoS-атак
- Уязвимостей переполнения буфера в реализации SSL/TLS
- Инициаций хэндшейка SSL/TLS с неавторизованных машин (хотя такие хэндшейки в конце концов не будут аутентифицированы, `tls-auth` может их отсесть намного раньше)

Использование `tls-auth` требует, чтобы вы сгенерировали закрытый ключ общего пользования, который используется дополнительно к сертификатам/ключам ГОСТ:

```
openvpn --genkey --secret ta.key
```

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Эта команда сгенерирует статический ключ «OpenVPN-ГОСТ» и запишет его в файл `ta.key`. Этот ключ следует скопировать через уже существующий безопасный канал на сервер и все клиентские машины. Он может быть помещен в тот же каталог, что и файлы `ГОСТ.key` и `.crt`.

В серверной конфигурации добавьте:

```
tls-auth ta.key 0
```

В клиентской конфигурации добавьте:

```
tls-auth ta.key 1
```

7.4.2 user/group (кроме ОС Windows)

«OpenVPN-ГОСТ» была очень тщательно создана так, чтобы позволить отказаться от прав привилегированного пользователя после инициализации, и эту возможность следует всегда использовать в Linux/BSD/Solaris. Без прав привилегированного пользователя, работающий серверный демон «OpenVPN-ГОСТ» представляет собой значительно менее привлекательную цель для атакующего.

Чтобы отключить права привилегированного пользователя после инициализации, добавьте в серверную конфигурацию директивы:

```
user nobody
group nobody
```

7.4.3 Непривилегированный режим (только в Linux)

В Linux «OpenVPN-ГОСТ» может работать вообще без привилегий. Эта конфигурация несколько посложнее, но предоставляет наилучшую защиту.

Чтобы работать с этой конфигурацией, «OpenVPN-ГОСТ» следует сконфигурировать для работы с интерфейсом `iproute`, это делается указанием `-enable-iproute2` конфигурационному скрипту. Пакет `sudo` также должен быть доступен в вашей системе.

Эта конфигурация использует способность Linux менять права на устройство `tun`, так чтобы непривилегированный пользователь мог его использовать. Она также использует `sudo`, чтобы выполнить `iproute`, чтобы можно было модифицировать свойства интерфейса и таблицы маршрутизации.

Конфигурирование «OpenVPN-ГОСТ» :

- Напишите следующий скрипт и поместите его в `/usr/local/sbin/unpriv-ip`:

```
#!/bin/sh
sudo /sbin/ip $*
```

- Отредактируйте файл `/etc/sudoers`, добавив в него следующее, чтобы позволить пользователю `user1` выполнять `/sbin/ip`:

```
user1 ALL=(ALL) NOPASSWD: /sbin/ip
```

Вы также можете позволить группу пользователей следующей командой:

```
%users ALL=(ALL) NOPASSWD: /sbin/ip
```

- Добавьте следующее в вашу конфигурацию «OpenVPN-ГОСТ» :

```
dev tunX/tapX
iproute /usr/local/sbin/unpriv-ip
```

Пожалуйста, обратите внимание, что вы должны выбрать постоянную `X` и указать `tun` или `tap`, но не и то и другое.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

- В качестве привилегированного пользователя добавьте постоянный интерфейс и разрешите пользователю и/или группе управлять им, следующая команда создает tunX (замените вашим собственным) и позволяет user1 и группе пользователей использовать его.

```
openvpn --mktun --dev tunX --type tun --user user1 --group users
```

- Запустите «OpenVPN-ГОСТ» в контексте непривилегированного пользователя.

Дальнейшее усиление безопасности может быть добавлено путем исследования параметров в скрипте /usr/local/sbin/unpriv-ip .

7.4.4 chroot (кроме ОС Windows)

Директива chroot позволяет вам запереть демон «OpenVPN-ГОСТ» в так называемую тюрьму chroot, где демон не сможет работать ни с какими частями файловой системы в операционной системе, за исключением специального каталога, указанного как параметр к директиве. Например

```
chroot jail
```

заставит демон «OpenVPN-ГОСТ» перейти в подкаталог jail при инициализации, а затем переориентирует его корневую файловую систему в этот каталог, так что затем демону будет невозможно увидеть никаких файлов снаружи каталога jail и его подкаталогов. Это важно с точки зрения безопасности, потому что даже если атакующий сможет скомпрометировать сервер с помощью вредоносного кода, этот код будет заперт от большей части файловой системы сервера.

Предупреждения: поскольку chroot переориентирует файловую систему (только с точки зрения демона), необходимо поместить все файлы, которые могут потребоваться «OpenVPN-ГОСТ» после инициализации, в каталог jail, например, файл cri-verify или каталог client-config-dir.

7.4.5 Хранение корневого ключа (ca.key) на отдельной машине без сетевого соединения

Одно из преимуществ использования РКІ по стандарту X.509 с точки зрения безопасности состоит в том, что корневой ключ удостоверяющего центра (ca.key) не должен присутствовать на серверной машине «OpenVPN-ГОСТ» . В среде высокой безопасности вы можете захотеть специально выделить машину для целей подписания ключей, держать эту машину физически хорошо защищенной и отключить ее от всех сетей. Для переноса ключей можно использовать гибкие диски. Такие меры делают кражу корневого ключа исключительно трудной для атакующего, если только он не украдет физически машину для подписывания ключей.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8 Приложение. Список опций команды openvpn

8.1 Общие опции

«OpenVPN-ГОСТ» позволяет помещать любую опцию в командную строку или в конфигурационный файл. Хотя все опции командной строки имеют префикс в виде двойного дефиса, этот префикс может быть опущен, когда опцию помещают в конфигурационный файл.

-help	Показать опции
-config file	<p>Загрузить дополнительные конфигурационные опции из файла file, где каждая строка соответствует одной опции командной строки, но с опущенным двойным дефисом.</p> <p>Если -config file - единственная опция в команде openvpn, -config можно опустить и записать команду как openvpn file</p> <p>Заметьте, что конфигурационные файлы могут быть вложенными до осмысленной глубины.</p> <p>Можно использовать двойные или одинарные кавычки для ограничения параметров, включающих пробел, # или ; символы в первой колонке можно использовать для обозначения комментариев.</p> <p>Заметьте, что «OpenVPN-ГОСТ» обрабатывает escape-последовательности на основе обратной косой черты для символов, не заключенных в одинарные кавычки, так что следует иметь в виду следующие обозначения:</p> <p>\\ Обозначает одну обратную косую черту (\)</p> <p>\ " Передает буквально двойные кавычки, не интерпретируя их как ограничение параметра</p> <p>\ [SPACE] передает буквально пробел или табуляцию, не интерпретируя их как разделение параметров</p> <p>Например, в Windows используйте двойные обратные косые черты для представления путей к файлам:</p> <pre>secret "c:\\OpenVPN\\secret.key"</pre>

8.2 Туннельные опции

-mode m	Устанавливает режим работы OpenVPN. По умолчанию «OpenVPN-ГОСТ» работает в режиме точка-в-точку (p2p). В «OpenVPN-ГОСТ» присутствует режим «сервер», реализующий многоклиентную способность сервера.
-local host	Имя или IP-адрес локального хоста для связывания. Если указан, «OpenVPN-ГОСТ» будет связываться только с этим адресом. Если не указан, «OpenVPN-ГОСТ» будет связываться со всеми интерфейсами.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-remote host [port][proto]</code></p>	<p>Имя или IP-адрес удаленного хоста. На клиенте для надежности могут быть указаны несколько опций <code>-remote</code>, каждая относится к отдельному серверу OpenVPN. Указание нескольких опций <code>-remote</code> для этой цели - отдельный случай более общей функциональности профиля соединения. См. ниже описание <code><connection></code>.</p> <p>Клиент OpenVPN будет пытаться соединиться с серверами на <code>host:port</code> в порядке, указанном в списке опций <code>-remote</code>. <code>proto</code> указывает, какой протокол использовать при соединении с удаленным хостом, и в случае «OpenVPN-ГОСТ» может быть только <code>tcp</code> при работе с алгоритмами ГОСТ, и <code>tcp</code> или <code>udp</code> в остальных случаях.</p> <p>Клиент перейдет к следующему хосту в списке, если соединение с предыдущим установить не удастся. Обратите внимание, что в любой момент времени клиент OpenVPN может быть соединен только с одним сервером.</p> <p>Обратите внимание на следующий предельный случай. Если вы используете опции <code>-remote</code> И отказываетесь от прав привилегированного пользователя с помощью <code>-user</code> и/или <code>-group</code>, И клиент работает не в Windows, если клиенту нужно переподключиться к другому серверу, и этот сервер передает различные настройки TUN/TAP или маршрутизации, клиенту может не хватить необходимых прав, чтобы закрыть и снова открыть интерфейс TUN/TAP. Это может привести к прекращению работы клиента с фатальной ошибкой.</p> <p>Если опция <code>-remote</code> не указана, «OpenVPN-ГОСТ» будет слушать пакеты с любого IP-адреса, но не будет обрабатывать эти пакеты, если они не пройдут все аутентификационные тесты. Это требование к аутентификации относится ко всем потенциальным партнерам, даже приходящим с известных и предположительно доверенных IP-адресов.</p> <p>При использовании в режиме TCP, <code>-remote</code> будет работать как фильтр, отвергая соединения со всех хостов, не соответствующих значению параметра <code>host</code>.</p> <p>Если значение параметра <code>host</code> - DNS-имя, которое разрешается в несколько IP-адресов, один из них будет выбран случайно, предоставляя своего рода возможность уравнивания нагрузки.</p>
--	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><connection></p>	<p>Определяет профиль клиентского соединения. Профили клиентского соединения - группы опций «OpenVPN-ГОСТ», описывающие, как связаться с конкретным сервером OpenVPN. Профили клиентского соединения указываются в конфигурационном файле «OpenVPN-ГОСТ», и каждый профиль начинается с <connection> и заканчивается </connection>.</p> <p>Клиент OpenVPN будет пробовать каждый профиль соединения последовательно, пока не достигнет успешного соединения.</p> <p>Опция <code>-remote-random</code> может использоваться для того, чтобы с самого начала «смешать» список соединений.</p> <p>Вот пример использования профилей соединений:</p> <pre>client dev tun <connection> remote 198.19.34.56 1194 tcp </connection> <connection> remote 198.19.34.56 443 tcp </connection> <connection> remote 198.19.34.56 443 tcp http-proxy 192.168.0.8 8080 http-proxy-retry </connection> <connection> remote 198.19.36.99 443 tcp http-proxy 192.168.0.8 8080 http-proxy-retry </connection> persist-key persist-tun pkcs12 client.p12 ns-cert-type server verb 3</pre> <p>Сначала мы пытаемся соединиться с сервером на 198.19.34.56:1194, используя TCP. Если это не удастся, мы пытаемся соединиться с 198.19.34.56:443, используя TCP, и далее по порядку.</p>
---------------------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>Внутри блока <connection> могут быть следующие опции «OpenVPN-ГОСТ» :</p> <p>bind, connect-retry, connect-retry-max, connect-timeout, float, http-proxy, http-proxy-option, http-proxy-retry, http-proxy-timeout, local, lport, nobind, port, proto, remote, rport, socks-proxy, and socks-proxy-retry.</p> <p>Существует механизм умолчания для указания опций, применимых ко всем профилям <connection>. Если любая из вышеуказанных опций (за исключением remote) появляется вне блока <connection>, но в конфигурационном файле, содержащем хотя бы один блок <connection>, эта опция будет использована по умолчанию для всех блоков <connection>, которые следуют за ней в конфигурационном файле.</p> <p>Например, предположим, что опция nobind помещена в начало приведенного выше конфигурационного файла, перед первым блоком <connection>. Эффект будет такой же, как если бы nobind была объявлена во всех блоках <connection> под ней.</p>
-remote-random	<p>Когда указаны несколько адресов/портов remote, или если используются профили соединения, данная опция изначально рандомизирует порядок списка в качестве своего рода простейшей меры равномерного распределения нагрузки.</p>
-proto p	<p>Использовать протокол p для связи с удаленным хостом. p может быть udp, tcp-client или tcp-server.</p> <p>Умолчательный протокол - udp, если опция -proto не указана.</p> <p>Для работы по UDP опция -proto udp должна быть указана у обоих партнеров.</p> <p>Для работы по TCP один из соединяющихся должен использовать -proto tcp-server и второй должен использовать -proto tcp-client. Партнер, начавший с tcp-server, будет бесконечно ждать входящего соединения. Партнер, начавший с tcp-client, попытается подключиться, и если не удастся, будет спать 5 секунд (это время можно изменить с помощью опции -connect-retry) и будет опять пытаться подключиться бесконечное количество раз или до N повторений (количество повторений можно изменить с помощью опции -connect-retry-max). И клиент, и сервер будут симулировать сигнал рестарта SIGUSR1, если какая-либо из сторон будет пересоединяться.</p>
-connect-retry n	<p>Для -proto tcp-client, ждать n секунд между попытками переприсоединиться (по умолчанию 5).</p>
-connect-retry-max n	<p>Для -proto tcp-client, пытаться переподключиться n раз (бесконечное количество раз по умолчанию).</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–auto-proxy</p>	<p>Попытаться автоматически почувствовать настройки HTTP или SOCKS-прокси. Если никаких настроек нет, будет произведена попытка прямого соединения. Если присутствуют и HTTP, и SOCKS-настройки, будет предпочтен HTTP. Если HTTP-прокси-сервер требует пароля, он будет запрошен со стандартного входа или через интерфейс управления. Если операционная система не поддерживает API для возвращения настроек прокси, будет произведена попытка установить прямое соединение. В настоящее время только клиенты Windows поддерживают эту опцию через InternetQueryOption API.</p>
<p>–http-proxy server port [authfile 'auto'] 'auto-nct' auth-method]</p>	<p>Соединиться с удаленным хостом через HTTP-прокси с адресом server и портом port. Если требуется HTTP Proxy-Autenticate, authfile - файл, содержащий логин и пароль на 2 строках, или «stdin» для запроса с консоли. auth-method должен быть «none», «basic» или «ntlm». HTTP-дайджест-аутентификация также поддерживается, но только через флаги auto или auto-nct (см. ниже). Флаг auto заставляет «OpenVPN-ГОСТ» автоматически определять auth-method и запрашивать со стандартного входа или интерфейса управления логин и пароль, если требуются. Флаг auto-nct (no clear-text auth) велит «OpenVPN-ГОСТ» автоматически определять метод аутентификации, но отвергать слабые аутентификационные протоколы, такие как HTTP-аутентификация Basic.</p>
<p>–http-proxy-retry</p>	<p>Бесконечно пытаться переприсоединиться при ошибках HTTP-прокси. Если происходит такая ошибка, симулировать SIGUSR1.</p>
<p>–http-proxy-timeout n</p>	<p>Установить таймаут прокси в n секунд, по умолчанию 5.</p>
<p>–http-proxy-option type[parm]</p>	<p>Установить расширенные опции HTTP-прокси. Повторить, чтобы установить несколько опций. VERSION version - Установить номер версии HTTP в version (по умолчанию 1.0). AGENT user-agent - Установить HTTP-строку "User-Agent" в user-agent</p>
<p>–socks-proxy server [port]</p>	<p>Подключиться к удаленному хосту через Socks-прокси с адресом server и портом port (по умолчанию 1080).</p>
<p>–socks-proxy-retry</p>	<p>Бесконечно пытаться подключиться при ошибках Socks-прокси. Если случается ошибка Socks-прокси, симулировать SIGUSR1.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-resolv-retry n</p>	<p>Если разрешение имени хоста для -remote оказывается ошибочным, попытаться разрешить в течение n секунд перед ошибкой. Установить n в infinite, чтобы пытаться разрешить бесконечно. По умолчанию установлена -resolve-retry infinite. Можно отключить эту опцию, установив n=0.</p>
<p>-float</p>	<p>Позволить удаленному партнеру менять свой IP-адрес и/или номер порта, например, из-за DHCP (это умолчание, если -remote не используется.) -float, указанный вместе с -remote, позволяет сеансу OpenVPN изначально подключаться к партнеру с известным адресом, однако если пакеты приходят с нового адреса и проходят аутентификационные тесты, новый адрес примет управление сеансом. Это полезно, когда вы соединяетесь с партнером с динамическим адресом, например, пользователем с телефона или клиентом DHCP. В сущности, -float велит «OpenVPN-ГОСТ» принимать аутентифицированные пакеты с любого адреса, а не только с того, который указан в опции -remote.</p>
<p>-ipchange cmd</p>	<p>Выполнить команду оболочки cmd, когда наш удаленный ip-адрес с самого начала аутентифицирован или изменяется. Выполнять как: cmd ip_address port_number Не используйте -ipchange в режиме -mode server. Вместо этого воспользуйтесь скриптом -client-connect. См. в разделе «Переменные среды» ниже дополнительные параметры, передаваемые как переменные среды. Обратите внимание, что cmd может быть командой оболочки с несколькими аргументами, в этом случае все аргументы, генерированные «OpenVPN-ГОСТ», будут добавлены в конец строки cmd, чтобы создать командную строку, которая будет передана в скрипт. Если вы работаете в среде с переменным IP-адресом, где IP-адреса каждого партнера могут меняться без предупреждения, вы можете использовать этот скрипт, например, чтобы редактировать файл /etc/hosts с текущим адресом партнера. Скрипт будет выполняться каждый раз, когда удаленный партнер меняет свой IP-адрес. Подобным же образом, если <i>наш</i> IP-адрес меняется из-за DHCP, нам следует сконфигурировать наш скрипт перемены IP-адреса так, чтобы «OpenVPN-ГОСТ» получала сигнал SIGHUP или SIGUSR1. «OpenVPN-ГОСТ» затем переустанавливает соединение со своим последним аутентифицированным партнером на его новом IP-адресе.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

-port port	Номер TCP-порта для локального и удаленного хостов. Текущий номер по умолчанию 1194 представляет официальное назначение порта IANA для OpenVPN.
-lport port	Номер TCP-порта для связывания.
-rport port	Номер TCP-порта для удаленного хоста.
-bind	Связаться с локальным адресом и портом. Это умолчание, если не используются какие-либо из опций -proto tcp-client, -http-proxy или -socks-proxy.
-nobind	Не связываться с локальным адресом и портом. IP-стек назначит динамический порт для возвращающихся пакетов. Поскольку значение динамического порта партнеру неизвестно заранее, эта опция подходит только для партнеров, которые будут инициировать соединение, используя опцию -remote.
-dev tunX tapX null	Виртуальное сетевое устройство TUN/TAP (для динамического устройства X можно опустить.) Вы должны использовать на обоих концах соединения либо устройства tun, либо tap. Вы не можете указывать на одном конце tap, а на другом tun, поскольку они представляют различные слои сети. Устройства tun инкапсулируют IPv4 или IPv6 (слой 3 OSI), а устройства tap инкапсулируют Ethernet 802.3 (слой 2 OSI).
-dev-type device-type	Какой тип устройства мы используем? device-type должен иметь значение tun (слой 3 OSI) или tap (слой 2 OSI). Используйте эту опцию только в том случае, если устройство TUN/TAP, использованное в опции -dev, не начинается с tun или tap.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-topology mode</p>	<p>Сконфигурировать виртуальную адресную топологию, работая в режиме -dev tun. Эта директива не имеет значения в режиме -dev tap, который всегда использует топологию subnet. Если вы настраиваете эту директиву на сервере, директивы -server и -server-bridge автоматически передадут выбранные вами настройки топологии клиентам. Эту директиву также можно передать клиентам вручную. Как и директива -dev, эта директива должна всегда быть совместимой между клиентом и сервером.</p> <p>mode может иметь значение:</p> <p>net30 - использовать топологию точка-в-точку, назначая одну подсеть /30 каждому клиенту. Это предназначено для того, чтобы разрешить семантику точка-в-точку, когда несколько или все подключающиеся клиенты могут быть ОС Windows. Это умолчание.</p> <p>r2r - использовать топологию точка-в-точку, где удаленная конечная точка интерфейса tun клиента всегда указывает на локальную конечную точку интерфейса tun сервера. Этот режим назначает один IP-адрес для каждого соединяющегося клиента. Используйте только тогда, когда ни один из подключающихся клиентов не является ОС Windows.</p> <p>subnet - используйте подсеть вместо топологии точка-в-точку, сконфигурировав интерфейс tun с локальным IP-адресом и маской подсети, подобным топологии, используемой в -dev tap и режиме «мост» Ethernet. Этот режим назначает один IP-адрес каждому соединяющемуся клиенту и работает в Windows и в Unix-подобных системах. При использовании в Windows требует версию драйвера TAP-WIN32 8.2 или выше. При использовании в Unix-подобных системах, требует, чтобы драйвер tun поддерживал команду ifconfig, которая устанавливает подсеть вместо удаленного конечного IP-адреса.</p>
<p>-tun-ipv6</p>	<p>Построить tun-связь, способную передавать трафик по протоколу IPv6. Следует использовать совместно с -dev tun или -dev tunX. Если никакой специальной поддержки IPv6 в TUN для вашей операционной системы не скомпилировано в «OpenVPN-ГОСТ», будет выводиться предупреждение.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-dev-node node</p>	<p>Явным образом установить узел устройства, а не использовать /dev/net/tun, /dev/tun, /dev/tap и т.д. Если «OpenVPN-ГОСТ» не может определить, является ли node устройством TUN или TAP, на основании этого имени, вы должны также указать -dev type tun или -dev type tap.</p> <p>В системах Windows выберите адаптер TAP-Win32, который называется node, в Network Connections Control Panel или GUID адаптера в скобках. В Windows можно также использовать опцию -show-adapters, чтобы пронумеровать все доступные адаптеры TAP-Win32, эта опция покажет название контрольной панели сетевых соединений и GUID для каждого адаптера TAP-Win32.</p>
<p>-laddr address</p>	<p>Указать адрес слоя связи, более известный как MAC-адрес. Применяется только к устройствам TAP.</p>
<p>iproute cmd</p>	<p>Установить альтернативную команду для выполнения вместо умолчательной команды iproute2. Может быть использована, чтобы выполнять «OpenVPN-ГОСТ» в непривилегированной среде.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-ifconfig l rn</p>	<p>Установить параметры адаптера TUN/TAP. l - IP-адрес локальной конечной точки VPN. Для устройств TUN, rn - IP-адрес удаленной конечной точки VPN. Для устройств TAP, rn - маска подсети виртуального сегмента Ethernet, который создается или с которым связываются.</p> <p>Для устройств TUN, которые упрощают виртуальные IP-соединения точка-в-точку, правильное использование – ifconfig - использовать два частных IP-адреса, которые не являются членами какой-либо используемой существующей подсети. IP-адреса могут идти подряд, и их порядок у удаленного партнера должен быть обратным. После того, как VPN установлена, вы будете отправлять сигнал ping на rn через VPN.</p> <p>Для устройств TAP, которые предоставляют возможность создавать виртуальные сегменты Ethernet, -ifconfig используется, чтобы настроить IP-адрес и маску подсети так же, как был бы подобным образом сконфигурирован физический адаптер Ethernet. Если вы пытаетесь соединиться с удаленным Ethernet-«мостом», IP-адрес и подсеть следует установить в величины, которые были бы действительны в сегменте Ethernet, с которым вы соединяетесь (обратите также внимание, что для этой же цели можно использовать DHCP).</p> <p>Эта опция, изначально прокси для команды ifconfig, предназначена, чтобы упростить туннельную конфигурацию TUN/TAP, предоставляя стандартный интерфейс различным реализациям ifconfig на различных платформах.</p> <p>Параметры -ifconfig, которые являются IP-адресами, также могут быть указаны как имя, разрешимое в DNS или в файл /etc/hosts.</p> <p>Для устройств TAP, -ifconfig не следует использовать, если интерфейс TAP будет получать аренду IP-адреса с сервера DHCP.</p>
<p>-ifconfig-поехес</p>	<p>Не выполнять команды ifconfig/netsh, вместо этого передавать параметры -ifconfig в скрипты, используя переменные среды.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–ifconfig-nowarn</p>	<p>Не выводить предупреждение о проверке корректности опций, если опция –ifconfig на этой стороне соединения не соответствует удаленной стороне. Это полезно, когда вы хотите сохранить общие преимущества проверки корректности опций (см. также опцию –disable-осс), отключая только компонент проверки ifconfig.</p> <p>Например, если у вас есть конфигурация, где локальный хост использует -ifconfig, но удаленный хост ее не использует, примените –ifconfig-nowarn на локальном хосте.</p> <p>Эта опция также отключит предупреждения о потенциальных конфликтах адресов, которые иногда раздражают более опытных пользователей включением «ложных положительных» предупреждений.</p>
<p>–route network/IP [netmask] [gateway] [metric]</p>	<p>Добавить маршрут в таблицу маршрутов после того, как установлено соединение. Можно указать несколько маршрутов. Маршруты будут автоматически отключены в обратном порядке перед отключением устройства TUN/TAP.</p> <p>Эта опция предназначена как прокси для удобства пользования командой оболочки route, в то же время предоставляя семантику, переносимую через пространство платформы «OpenVPN-ГОСТ» .</p> <p>netmask по умолчанию - 255.255.255.255</p> <p>gateway по умолчанию - берется из –route-gateway или второго параметра –ifconfig, когда указан –dev tun.</p> <p>metric по умолчанию - берется из –route-metric, в остальных случаях 0.</p> <p>Умолчание можно указать, оставив опцию пустой или указав значение «default».</p> <p>Параметры network и gateway могут также быть указаны как имя, разрешаемое в DNS или файл /etc/hosts, или как одно из трех специальных ключевых слов.</p> <p>vpn_gateway - адрес удаленной конечной точки VPN (берется или из –route-gateway или из второго параметра –ifconfig, если указана опция –dev tun)</p> <p>net_gateway - ранее существовавший гейт с умолчательным IP, читается из таблицы маршрутизации (поддерживается не во всех ОС)</p> <p>remote_host - адрес –remote, если «OpenVPN-ГОСТ» работает в клиентском режиме и не определена в серверном режиме.</p>
<p>–max-routes n</p>	<p>Позволяет указать опции –route с максимальным количеством n, либо в локальном конфигурационном файле, либо взятые с сервера OpenVPN. По умолчанию n=100.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<code>-route-gateway gw 'dhcp'</code>	Указать умолчательный гейт gw для использования с <code>-route</code> . Если в качестве параметра указано <code>dhcp</code> , адрес гейта будет взят из взаимодействия DHCP с серверной локальной сетью «OpenVPN-ГОСТ» .
<code>-route-metric m</code>	Указать умолчательную метрику m для использования с <code>-route</code> .
<code>-route-delay [n] [w]</code>	Подождать n секунд (по умолчанию 0) после установки соединения, прежде чем добавлять маршруты. Если n равно 0, маршруты будут добавлены немедленно после установления соединения. Если опция <code>-route-delay</code> опущена, маршруты будут добавлены сразу после открытия устройства TUN/TAP и выполнения скрипта <code>-up</code> , перед отключением любых прав привилегированного пользователя директивами <code>-user</code> или <code>-group</code> (или выполнения <code>-chroot</code>). Эта опция полезна в сценариях, где используется DHCP для установки адресов адаптера tap. Задержка даст хендшейку DHCP время завершиться, прежде чем будут добавлены маршруты. В Windows опция <code>-route-delay</code> пытается быть более интеллектуальной, ожидая w секунд (по умолчанию w=30) включения адаптера TAP-Win32 перед добавлением маршрутов.
<code>-route-up cmd</code>	Выполнить команду оболочки cmd после того, как маршруты добавлены в соответствии с опцией <code>-route-delay</code> . См. в разделе «Переменные среды» ниже дополнительные параметры, которые передаются как переменные среды. Обратите внимание, что cmd может быть командой оболочки с несколькими аргументами.
<code>-route-noexec</code>	Не добавлять и не удалять маршрутов автоматически. Вместо этого передавать маршруты в скрипт <code>-route-up</code> с помощью переменных среды.
<code>-route-nopull</code>	При использовании с <code>-client</code> или <code>-pull</code> , принять опции, переданные сервером, КРОМЕ маршрутов. При использовании на клиенте эта опция эффективно запрещает серверу добавлять маршруты в таблицу маршрутизации клиента, однако обратите внимание, что эта опция все же позволяет серверу устанавливать свойства TCP/IP на клиентском интерфейсе TUN/TAP.
<code>-allow-pull-fqdn</code>	Позволяет клиенту брать DNS-имена с сервера (вместо того, чтобы ограничиться IP-адресом) для <code>-ifconfig</code> , <code>-route</code> и <code>-route-gateway</code> .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-redirect-gateway flags...</p>	<p>(Экспериментальная) Автоматически выполняет команды маршрутизации, чтобы заставить весь исходящий трафик проходить через VPN.</p> <p>Эта опция выполняет три шага:</p> <ol style="list-style-type: none"> 1) Создает статический маршрут для адреса -remote, который форвардится на ранее существовавший умолчательный гейт. Это делается для того, чтобы третий шаг не создал маршрутизационной петли. 2) Удаляет маршрут умолчательного гейта. 3) Устанавливает новый умолчательный гейт в качестве конечной точки VPN (берется либо из -route-gateway, либо из второго параметра -ifconfig, если указана опция -dev tun). <p>Когда туннель разрывается, все вышеизложенные шаги выполняются в обратном порядке, чтобы восстановить исходный умолчательный маршрут.</p> <p>Флаги опции:</p> <p>local - добавьте флаг local, если оба сервера OpenVPN прямо соединены через общую подсеть, например, беспроводную. Флаг local заставит опустить вышеописанный шаг 1.</p> <p>def1 - используйте этот флаг, чтобы переопределить умолчательный гейт, используя 0.0.0.0/1 и 128.0.0.0/1 вместо 0.0.0.0/0. Это имеет то преимущество, что исходный умолчательный гейт переопределяется, но не уничтожается.</p> <p>bypass-dhcp - добавляет прямой маршрут к серверу DHCP (если он не локальный), который обходит туннель (доступно на клиентах Windows, может быть недоступно на других клиентах)</p> <p>bypass-dns - добавляет прямой маршрут к серверу (серверам) DNS (если они не локальные), который обходит туннель (доступно на клиентах Windows, может быть недоступно на других клиентах)</p> <p>Настоятельно рекомендуется использование флага def1.</p>
-----------------------------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–tun-mtu n</p>	<p>Принять MTU устройства TUN за n и вычислить из него MTU связи (умолчание=1500). В большинстве случаев вы, вероятно, захотите оставить этот параметр установленным в умолчательное значение.</p> <p>MTU (Maximum Transmission Unit) - максимальный размер пакета в байтах, который может быть отправлен без фрагментирования по конкретному пути в сети. «OpenVPN-ГОСТ» требует, чтобы пакеты по контрольным каналам или каналам данных пересылались без фрагментирования.</p> <p>Проблемы с MTU часто проявляются как соединения, которые обрываются во время периодов активного использования.</p> <p>Лучше использовать опции –fragment и/или –mssfix, чтобы справиться с проблемами размеров MTU.</p>
<p>–tun-mtu-extra n</p>	<p>Предположить, что устройство TUN/TAP может вернуть пакет на n байтов больше, чем размер, указанный в –tun-mtu. Этот параметр по умолчанию установлен в 0, что достаточно для большинства устройств TUN. Устройства TAP могут ввести дополнительное увеличение размера MTU, поэтому когда используются устройства TAP, используется умолчательное значение 32. Этот параметр контролирует только размеры внутреннего буфера «OpenVPN-ГОСТ», так что никакого увеличения передачи, связанного с использованием большей величины, не происходит.</p>
<p>–mtu-disc type</p>	<p>Следует ли нам выполнять Path MTU discovery на TCP-канале? Поддерживается только в таких ОС как Linux, которые поддерживают необходимый системный вызов для настройки.</p> <p>'no' - Никогда не посылать фреймы DF (Don't Fragment)</p> <p>'maybe' - использовать инструкции, связанные с маршрутом</p> <p>'yes' - Всегда DF (Don't Fragment)</p>
<p>–mtu-test</p>	<p>Чтобы эмпирически замерить MTU в начале соединения, добавьте опцию –mtu-test к вашей конфигурации. «OpenVPN-ГОСТ» отправит пинговые пакеты разных размеров удаленному партнеру и измерит самые большие пакеты, которые были успешно получены. Процесс –mtu-test обычно занимает около 3 минут.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-fragment max</p>	<p>Включает внутреннюю фрагментацию датаграмм, так чтобы не посылались UDP-датаграммы размером больше, чем max байтов.</p> <p>Параметр max интерпретируется так же, как параметр -link-mtu, т.е. был добавлен размер UDP-пакета после инкапсуляции, но без самого UDP-заголовка.</p> <p>Опция fragment имеет смысл только в том случае, если вы пользуетесь протоколом UDP (-proto udp).</p> <p>-fragment добавляет 4 байта к каждой датаграмме.</p> <p>См. в описании опции mssfix внизу описание важной опции, связанной с -fragment.</p> <p>Следует также иметь в виду, что эта опция не предназначена для того, чтобы заменить UDP-фрагментацию на уровне IP-стека. Она введена как последнее средство, когда path MTU discovery недоступно. Использование этой опции менее эффективно, чем восстановление открытия MTU-пути для вашей IP-связи и использования собственной IP-фрагментации. Но бывают обстоятельства, когда использование возможностей OpenVPN по внутренней фрагментации могут быть вашей единственной возможностью, например, передача по туннелю мультикастового потока UDP, требующего фрагментации.</p>
----------------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–mssfix max</p>	<p>Объявить сеансам TCP, работающим через туннель, что им следует ограничить размеры отправляемых пакетов так, чтобы после того, как «OpenVPN-ГОСТ» их инкапсулировала, размер результирующих UDP-пакетов, которые «OpenVPN-ГОСТ» посылает своему партнеру, не будет превосходить max байтов.</p> <p>Параметр max интерпретируется так же, как параметр –link-mtu, т.е. был добавлен размер UDP-пакета после инкапсуляции, но без самого UDP-заголовка.</p> <p>Опция -mssfix имеет смысл только тогда, когда вы используете протокол UDP, т.е. –proto udp.</p> <p>–mssfix и –fragment в идеале следует использовать вместе, где –mssfix будет прежде всего пытаться сделать так, чтобы TCP не нуждалось в фрагментации пакетов, и если большие пакеты все равно проходят (с протоколов, отличных от TCP), –fragment их фрагментирует внутри VPN.</p> <p>И –fragment, и –mssfix предназначены для того, чтобы обходить случаи, когда Path MTU discovery недоступно на сетевом пути между партнерами, общающимися через «OpenVPN-ГОСТ» .</p> <p>Обычный симптом подобной проблемы - соединение OpenVPN, которое успешно начинается, но потом замирает во время активного использования.</p> <p>Если опции –fragment и –mssfix используются вместе, –mssfix берет умолчательное значение параметра max из опции –fragment max.</p> <p>Таким образом, можно уменьшить максимальный размер UDP-пакета до 1300 (хорошая начальная попытка для решения проблем соединения, связанных с MTU) со следующими опциями:</p> <p>–tun-mtu 1500 –fragment 1300 –mssfix</p>
<p>–sndbuf size</p>	<p>Устанавливает размер буфера отправления TCP/UDP-сокета. В настоящее время по умолчанию равно 65536 байтов.</p>
<p>–rcvbuf size</p>	<p>Устанавливает размер буфера получения TCP/UDP-сокета. В настоящее время по умолчанию равно 65536 байтов.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–socket-flags flags...</p>	<p>Применить данные флаги к транспортному сокету «OpenVPN-ГОСТ» . В настоящее время поддерживается только флаг TCP_NODELAY.</p> <p>Флаг TCP_NODELAY полезен в режиме TCP и заставляет ядро сразу же посылать туннельные пакеты через TCP-соединение, не пытаясь группировать несколько маленьких пакетов в один большой пакет. Это может привести к существенному уменьшению времени задержки.</p> <p>Эта опция может передаваться с сервера на клиент, и для максимального эффекта ее следует использовать и на сервере, и на клиенте.</p>
<p>–txqueuelen n</p>	<p>(Только для Linux) Установить длину очереди TX на интерфейсе TUN/TAP. В настоящее время по умолчанию равна 100.</p>
<p>–shaper n</p>	<p>Ограничивает ширину полосы пропускания исходящих туннельных данных в n байт в секунду на TCP/UDP порту. Если вы хотите ограничить ширину полосы пропускания в обе стороны, используйте эту опцию у обоих партнеров.</p> <p>«OpenVPN-ГОСТ» использует следующий алгоритм для реализации ограничения полосы пропускания трафика. При величине полосы пропускания в n байт в секунду, после того, как запись датаграммы в b байтов поставлена в очередь на TCP/UDP порту, подождать минимум (b/n) секунд, прежде чем ставить в очередь следующую запись.</p> <p>Следует заметить, что «OpenVPN-ГОСТ» поддерживает несколько туннелей между одними и теми же двумя партнерами, позволяя вам конструировать одновременно полноскоростные туннели и туннели с уменьшенной полосой пропускания, маршрутизируя низкоприоритетные данные по туннелям с уменьшенной полосой пропускания, а остальные данные по туннелю с полной скоростью.</p> <p>Заметьте также, что для туннелей с низкой полосой пропускания (меньше 1000 байтов в секунду) вам, вероятно, следует использовать более низкие значения MTU (см. выше), иначе время задержки пакетов так вырастет, что будет вызывать таймауты в слое TLS и в TCP-соединениях, работающих по туннелю.</p> <p>В «OpenVPN-ГОСТ» n разрешено находиться в пределах от 100 байт в секунду до 100 мегабайт в секунду.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-inactive n [bytes]</p>	<p>Заставляет «OpenVPN-ГОСТ» отключаться после n секунд неактивности устройства TUN/TAP. Время бездействия измеряется с последнего входящего туннельного пакета. Если включен опциональный параметр bytes, отключение после n секунд бездействия на устройстве tun/tap производит комбинированный подсчет байтов туда/обратно, который меньше, чем bytes.</p>
<p>-ping n</p>	<p>Отправляет сигнал ping на удаленный хост через контрольный TCP/UDP-канал, если никаких пакетов не было отправлено по крайней мере n секунд (укажите ping для обоих партнеров, чтобы пакеты ping отправлялись в обоих направлениях, поскольку пакеты ping в «OpenVPN-ГОСТ» не отражаются, как пакеты ping в IP). При использовании в одном из защищенных режимов OpenVPN (где указаны -secret, -tls-server или -tls-client) пакет ping будет криптографически защищен. Эта опция предназначена для двух вариантов использования:</p> <ol style="list-style-type: none"> 1) Совместимость с брандмауэрами, работающими на сеансовом уровне. Периодический сигнал ping обеспечит то, что такой брандмауэр, который позволяет UDP-пакетам проходить, не оборвет сеанс по таймауту. 2) Предоставить удаленному хосту основу для тестирования существования его партнера с использованием опции -ping-exit.
<p>-ping-exit n</p>	<p>Заставляет «OpenVPN-ГОСТ» завершать работу после того, как пройдут n секунд без получения пакета ping или другого пакета от удаленного хоста. Эта опция может использоваться совместно с -inactive, -ping и -ping-exit, чтобы создать двухрусное завершение работы в результате неактивности. Например</p> <pre>openvpn [options...] -inactive 3600 -ping 10 -ping-exit 60</pre> <p>использованное для обоих партнеров заставит OpenVPN завершить работу в течение 60 секунд, если партнер отсоединяется, и в течение часа, если не будет обмена никакими реальными туннельными данными.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–ping-restart n</p>	<p>Похоже на –ping-exit, но начинает перезапуск с сигналом SIGUSR1 после того, как пройдут n секунд без принятия пакета ping или другого пакета от удаленного хоста.</p> <p>Эта опция полезна в тех случаях, когда удаленный партнер имеет динамический IP-адрес, и для следования за IP-адресом используется DNS-имя с низким TTL с применением сервиса типа http://dyndns.org и динамического DNS-клиента, такого как ddclient.</p> <p>Если партнера невозможно достичь, начнется перезапуск, заставляющий имя хоста, использованное с –remote, перерезрешиться (если также указана опция –resolv-retry).</p> <p>В серверном режиме, –ping-restart, –inactive или любой другой вид внутреннего сигнала, всегда будет применяться к объектам индивидуальных клиентских экземпляров, а не к целому серверу. Также обратите внимание, что в серверном режиме любой внутренний сигнал, который в обычном случае вызовет перезапуск, вместо этого вызовет удаление объекта клиентского экземпляра.</p> <p>В клиентском режиме, параметр –ping-restart по умолчанию установлен в 120 секунд. Это умолчание будет действовать, пока клиент не получит другое значение с сервера, основанное на настройке –keepalive в серверной конфигурации. Чтобы отключить это умолчательное значение, установите на клиенте –ping-restart 0.</p> <p>См. в разделе сигналов внизу дополнительную информацию по SIGUSR1.</p> <p>Обратите внимание, что поведение SIGUSR1 может быть изменено опциями –persist-tun, –persist-key, –persist-local-ip и –persist-remote-ip.</p> <p>Также обратите внимание, что –ping-exit и –ping-restart - взаимоисключающие опции и не могут применяться совместно.</p>
<p>–keepalive n m</p>	<p>Директива, предназначенная для того, чтобы упростить выражение –ping и –ping-restart в конфигурациях серверного режима.</p> <p>Например, –keepalive 10 60 расшифровывается так:</p> <pre>if mode server: ping 10 ping-restart 120 push "ping 10" push "ping-restart 60" else ping 10 ping-restart 60</pre>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–ping-timer-rem</p>	<p>Запускать –ping-exit/–ping-restart только если у нас есть удаленный адрес. Используйте эту опцию, если вы запускаете демон в слушающем режиме (т.е. без определенного партнера –remote) и не хотите начинать подавать сигналы таймаутов, пока не соединится удаленный партнер.</p>
<p>–persist-tun</p>	<p>Не закрывать и не переоткрывать устройство TUN/TAP и не запускать скрипты при перезапусках SIGUSR1 или –ping-restart. SIGUSR1 - сигнал перезапуска, близкий к SIGHUP, но предлагающий более тонкий контроль над опциями перезапуска.</p>
<p>–persist-key</p>	<p>Не перечитывать ключевые файлы при SIGUSR1 или –ping-restart. Эту опцию можно совместить с –user nobody, чтобы позволять инициировать перезапуски сигналом SIGUSR1. Как правило, если вы отказываетесь от прав привилегированного пользователя в «OpenVPN-ГОСТ», демон не может быть перезапущен, потому что он теперь не сможет перечитать защищенные ключевые файлы. Эта опция решает проблему, запоминая прочитанные ключи при перезапусках SIGUSR1, так что их не нужно перечитывать.</p>
<p>–persist-local-ip</p>	<p>Сохранить изначально разрешенный местный IP-адрес и номер порта при перезапусках SIGUSR1 или –ping-restart.</p>
<p>–persist-remote-ip</p>	<p>Сохранить последний аутентифицированный удаленный IP-адрес и номер порта при перезапусках SIGUSR1 или –ping-restart.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-mlock</p>	<p>Отключает пейджинг, вызывая функцию mlockall из POSIX. Требуется, чтобы «OpenVPN-ГОСТ» изначально была запущена под привилегированным пользователем (хотя потом можно отказаться от прав привилегированного пользователя с помощью опции -user).</p> <p>Использование этой опции обеспечивает то, что ключевые и туннельные данные никогда не записываются на диск из-за операций пейджинга виртуальной памяти, которые происходят в большинстве современных операционных систем. Она обеспечивает то, что даже если атакующий смог взломать компьютер, на котором работает «OpenVPN-ГОСТ», он не сможет просканировать системный swap-файл, чтобы получить ранее использованные эфемерные ключи, которые используются в течение периода времени, определенного опциями -genepg (см. ниже), затем от них отказываются.</p> <p>Обратная сторона использования -mlock - то, что она уменьшит количество физической памяти, доступной другим приложениям.</p>
---------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-up cmd</p>	<p>Команда оболочки, которую следует выполнить после успешного открытия устройства TUN/TAP (до изменения UID – user). Скрипт up полезен для указания команд маршрутизации, которые маршрутизируют IP-трафик, предназначенный для частных подсетей, существующих на другом конце VPN-соединения, в туннель.</p> <p>Для -dev tun выполнять как: cmd tun_dev tun_mtu link_mtu ifconfig_local_ip ifconfig_remote_ip [init restart]</p> <p>Для -dev tap выполнять как: cmd tap_dev tap_mtu link_mtu ifconfig_local_ip ifconfig_netmask [init restart]</p> <p>См. в разделе «Переменные среды» ниже дополнительные параметры, которые передаются как переменные среды. Обратите внимание, что cmd может быть командой оболочки с несколькими аргументами, в этом случае аргументы, сгенерированные «OpenVPN-ГОСТ», будут добавлены в конец строки cmd, чтобы получить командную строку, которая будет передана в оболочку.</p> <p>Как правило, cmd запустит скрипт, чтобы добавить маршруты к туннелю.</p> <p>Как правило, после открытия устройства TUN/TAP вызывается скрипт up. В этом контексте последняя команда, которую параметр передал в скрипт, будет init. Если опция -up-restart также используется, скрипт up будет вызываться и для перезапусков. Перезапуск считается частичной переинициализацией «OpenVPN-ГОСТ», где сохраняется экземпляр TUN/TAP (это сохранение обеспечивает опция -persist-tun). Перезапуск может быть сгенерирован сигналом SIGUSR1, таймаутом -ping-restart или перезапуском соединения, когда опцией -proto запускается протокол TCP. Если происходит перезапуск, и была указана опция -up-restart, скрипт up будет вызван с restart в качестве последнего параметра.</p> <p>Следующий отдельный пример показывает, как скрипт -up может быть вызван в контексте и инициализации, и перезапуска (ПРИМЕЧАНИЕ: в целях безопасности, не запускайте этот пример, если UDP-порт 9999 не заблокирован вашим брандмауэром. Кроме того, пример будет выполняться бесконечно, так что его следует прервать с помощью control-c).</p> <pre>openvpn -dev tun -port 9999 -verb 4 -ping-restart 10 -up 'echo up' -down 'echo down' -persist-tun -up-restart</pre> <p>Обратите внимание, что «OpenVPN-ГОСТ» также предоставляет опцию -ifconfig, чтобы автоматически применить ifconfig к устройству TUN, исключая необходимость определять скрипт -up, если только вы не хотите также сконфигурировать маршруты в скрипте -up.</p>
----------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>Если <code>-ifconfig</code> также указана, «OpenVPN-ГОСТ» передаст локальный и удаленный конечные пункты команды <code>ifconfig</code> через командную строку в скрипт <code>-up</code>, так что они могут быть использованы, чтобы сконфигурировать маршруты, такие как: <code>route add -net 10.0.0.0 netmask 255.255.255.0 gw \$5</code></p>
<code>-up-delay</code>	<p>Отложить открытие TUN/TAP и возможное выполнение скрипта <code>-up</code> до тех пор, пока не установится TCP/UDP-соединение.</p> <p>В режиме <code>-proto udp</code> эта опция, как правило, требует использование <code>-ping</code>, чтобы дать возможность почувствовать инициацию соединения в отсутствие туннельных данных, поскольку UDP - «бессоединительный» протокол.</p> <p>В Windows эта опция отложит переход состояния TAP-Win32 в «подключенный», пока не установится соединение, т.е. пока не будет получен первый аутентифицированный пакет от партнера.</p>
<code>-down cmd</code>	<p>Команда оболочки, выполняемая после закрытия устройства TUN/TAP (после изменения UID <code>-user</code> и/или <code>chroot</code>). Вызывается с теми же параметрами и переменными среды, что и опция <code>-up</code>, описанная выше.</p> <p>Обратите внимание, что если вы снижаете права, пользуясь опциями <code>-user</code> и/или <code>group</code>, ваш скрипт <code>-down</code> также будет выполняться с пониженными правами.</p>
<code>-down-pre</code>	<p>Вызывать команду/скрипт <code>-down</code> до, а не после закрытия TUN/TAP.</p>
<code>-up-restart</code>	<p>Обеспечить возможность вызывать скрипты <code>-up</code> и <code>-down</code> для перезапусков, как и для изначального старта программы. Эта опция более подробно описана выше в описании опции <code>-up</code>.</p>
<code>-setenv name value</code>	<p>Настраивает измененную переменную среды <code>name=value</code> для передачи в скрипт.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–setenv FORWARD_COMPATIBLE 1</p>	<p>Ослабить проверку синтаксиса конфигурационного файла так, чтобы неизвестные директивы вызывали предупреждение, а не фатальную ошибку, в предположении, что данная неизвестная директива может быть действительной в будущих версиях «OpenVPN-ГОСТ» .</p> <p>Этой опцией следует пользоваться с осторожностью, потому что есть серьезные причины, связанные с безопасностью, заставляющие OpenVPN прекращать работу при проблемах в конфигурационном файле. Тем не менее есть причины желать, чтобы новые программные возможности не вызывали проблем при встрече со старыми программными версиями.</p>
<p>–setenv-safe name value</p>	<p>Установить измененную переменную среды OPENVPN_name=value для передачи в скрипт.</p> <p>Эта директива предназначена для передачи с сервера клиентам, и добавление префикса «OPENVPN_» к переменной среды - мера предосторожности, чтобы предотвратить атаку в стиле LD_PRELOAD от злонамеренного или скомпрометированного сервера.</p>
<p>–script-security level [method]</p>	<p>Эта директива предоставляет контроль над тем, как «OpenVPN-ГОСТ» использует внешние программы и скрипты, с политиками, определенными через уровни. Более низкие значения level накладывают больше ограничений, высокие - меньше. Настройки для level:</p> <p>0 - строго не вызывать внешних программ</p> <p>1 (по умолчанию) - вызывать только встроенные исполняемые файлы, такие как ifconfig, ip, route или netsh.</p> <p>2 - позволить вызывать встроенные исполняемые файлы, а также скрипты, определенные пользователем.</p> <p>3 - позволить передавать пароли в скрипты через переменные среды (вероятно небезопасно).</p> <p>Параметр method указывает, как OpenVPN следует вызывать внешние команды и скрипты. Настройки для method:</p> <p>execve - (по умолчанию) использовать функцию execve() в Unix-семействе операционных систем и CreateProcess() в Windows.</p> <p>system - использовать функцию system() (не рекомендуется и менее безопасно, поскольку командная строка внешней программы подлежит расширению оболочки).</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–disable-occ</p>	<p>Не выводить предупреждающее сообщение, если между партнерами обнаружены несоответствия опций. Пример несоответствия опций - если один из партнеров использует –dev tun, а второй –dev tap.</p> <p>Использовать эту опцию не рекомендуется, но она предоставляется в качестве временного решения в ситуациях, где «OpenVPN-ГОСТ» соединяется с OpenVPN более старой версии.</p>
<p>–user user</p>	<p>Изменяет ID пользователя в процессе «OpenVPN-ГОСТ» в user после инициализации, понижая права. Эта опция полезна, чтобы защитить систему в том случае, когда кто-то враждебный смог получить контроль над сеансом «OpenVPN-ГОСТ» . Хотя благодаря защите «OpenVPN-ГОСТ» это маловероятно, эта опция предоставляет дополнительное средство безопасности.</p> <p>Установив user в nobody или что-то такое же непривилегированное, вы ограничите вред, который может быть причинен враждебным агентом. Конечно, отняв права, вы не сможете их вернуть в сеансе «OpenVPN-ГОСТ» . Это значит, например, что если вы хотите перезапустить демон «OpenVPN-ГОСТ» с помощью сигнала SIGUSR1 (например, в ответ на перезапуск DHCP), вам следует воспользоваться одной или несколькими опциями –persist, чтобы обеспечить «OpenVPN-ГОСТ» отсутствие необходимости пользоваться какими-либо привилегированными операциями, чтобы перезапуститься (такими, как перечитывание ключевых файлов или запуск ifconfig на устройстве TUN).</p>
<p>–group group</p>	<p>Подобно опции –user, эта опция меняет ID группы в процессе «OpenVPN-ГОСТ» в group после инициализации.</p>
<p>–cd dir</p>	<p>Изменить каталог в dir перед чтением любых файлов, таких как конфигурационные файлы, ключевые файлы, скрипты и т.д. dir должен быть абсолютным путем, начинающимся с «/», и без каких-либо ссылок на текущий каталог, таких как «.» или «..».</p> <p>Эта опция полезна, когда вы запускаете «OpenVPN-ГОСТ» в режиме –daemon и хотите свести все ваши контрольные файлы OpenVPN в одном месте.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–chroot dir</p>	<p>Перейти в dir как в chroot после инициализации. –chroot, в сущности, переопределяет dir как верхний уровень каталога в дереве (/). «OpenVPN-ГОСТ» таким образом не сможет достичь никаких файлов вне этого дерева. Это может быть желательно с точки зрения безопасности.</p> <p>Поскольку операция chroot выполняется после инициализации, большинство опций «OpenVPN-ГОСТ», связанные с файлами, будут работать в контексте, предваряющем chroot. Во многих случаях параметр dir может указывать на пустой каталог, но могут появиться проблемы, когда после операции chroot выполняются скрипты или перезапуски.</p>
<p>–setcon context</p>	<p>Применить SELinux context после инициализации. Это, в сущности, предоставляет возможность ограничить права «OpenVPN-ГОСТ» до сетевых операций входа/выхода, благодаря SELinux. Эта опция идет дальше, чем –user и –chroot, потому что эти две опции, будучи прекрасными возможностями защиты, к сожалению, не защищают от повышения привилегий с помощью использования уязвимого системного вызова. Вы можете, конечно, использовать все три опции сразу, но пожалуйста имейте в виду, что поскольку setcon требует доступа в /proc, вам придется предоставлять его внутри каталога chroot (например, с помощью mount –bind).</p> <p>Поскольку операция setcon выполняется после инициализации, «OpenVPN-ГОСТ» может быть ограничена только системными вызовами, связанными с сетью, в то время как при использовании контекста перед запуском (таким, как предлагаемый в SELinux Reference Policies) вам придется позволить много вещей, требуемых только во время инициализации.</p> <p>Как и с chroot, могут возникнуть проблемы, когда после операции setcon выполняются скрипты или перезапуски, поэтому следует призадуматься над использованием опций –persist-key и –persist-tun.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-daemon [progname]</p>	<p>Стать демоном после завершения всех функций инициализации. Эта опция заставит все сообщения отправляться в файл syslog (такой как /var/log/messages) кроме вывода скриптов оболочки и команд ifconfig, которые будут отправляться в /dev/null, если их не перенаправить в другое место. Перенаправление в syslog происходит немедленно в момент, когда опция -daemon прочитывается в командной строке, хотя момент демонизации наступает позже. Если присутствует одна из опций -log, она заменит перенаправление в syslog.</p> <p>Опциональный параметр progname заставит «OpenVPN-ГОСТ» сообщить свое программное имя системному логгеру как progname. Это может быть полезно для связывания сообщений «OpenVPN-ГОСТ» в файле syslog со специальными туннелями. Если progname не указано, по умолчанию оно openvpn.</p> <p>Когда «OpenVPN-ГОСТ» запускается с опцией -daemon, она попытается отложить демонизацию до того момента, как завершится большинство инициализационных функций, способных к генерации фатальных ошибок. Это означает, что инициализационные скрипты могут протестировать возвращенный статус команды openvpn с достаточно надежным указанием того, была ли команда корректно инициализирована и вошла ли в петлю событий форвардинга пакетов.</p> <p>В «OpenVPN-ГОСТ» большая часть ошибок, происходящих после инициализации, не фатальны.</p>
<p>-syslog [progname]</p>	<p>Направлять вывод журнала в системный логгер, но не становиться демоном. См. в описании директивы -daemon, приведенном выше, описание параметра progname.</p>
<p>-passtos</p>	<p>Установить поле TOS туннельного пакета в то, чем является TOS информационного наполнения пакета.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-inetd</code> [wait nowait] [progname]</p>	<p>Используйте эту опцию, когда «OpenVPN-ГОСТ» работает на сервере inetd или xinetd.</p> <p>Опция wait/nowait должна соответствовать тому, что указано в конфигурационном файле ietd/xinetd. Режим nowait может быть использован только с <code>-proto tcp-server</code>. По умолчанию wait. Режим nowait может быть использован, чтобы представить демон OpenVPN как классический TCP-сервер, где запросы клиентских соединений обслуживаются на одном номере порта.</p> <p>Эта опция исключает использование опций <code>-daemon</code>, <code>-local</code> или <code>-remote</code>. Обратите внимание, что эта опция заставляет обрабатывать сообщения, в том числе об ошибках, так же, как опция <code>-daemon</code>. Опциональный параметр progname также обрабатывается точно так же, как в <code>-daemon</code>.</p> <p>Также обратите внимание, что в режиме wait каждый туннель OpenVPN требует отдельного TCP/UDP-порта и отдельного входа inetd или xinetd.</p>
<p><code>-log file</code></p>	<p>Выводить журнальные сообщения в file, включая вывод на стандартный вывод/стандартную ошибку, который генерируется вызванными скриптами. Если file уже существует, он будет обрезан. Эта опция активизируется немедленно, когда она прочитывается в командной строке, и заменит вывод в syslog, если также указаны <code>-daemon</code> или <code>-inetd</code>. Эта опция сохраняется в течение всей работы OpenVPN и не перезагружается SIGHUP, SIGUSR1 или <code>-ping-restart</code>.</p> <p>Обратите внимание, что в Windows, где OpenVPN запускается как сервис, журналирование происходит по умолчанию без необходимости указывать эту опцию.</p>
<p><code>-log-append file</code></p>	<p>Добавить журнальные сообщения к концу file. Если file не существует, он будет создан. Эта опция ведет себя точно также, как <code>-log</code>, за исключением того, что она приписывает сообщения к концу файла, а не обрезает его.</p>
<p><code>-suppress-timestamps</code></p>	<p>Избегать записи меток времени в журнальные сообщения, даже тогда, когда иначе они будут добавлены в начало. В особенности это прилагается к сообщениям журнала, направляемым в стандартный вывод.</p>
<p><code>-writepid file</code></p>	<p>Записать ID главного процесса «OpenVPN-ГОСТ» в file.</p>
<p><code>-nice n</code></p>	<p>Изменяет приоритет процесса после инициализации (n больше 0 - понижение приоритета, n меньше нуля - повышение приоритета).</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–fast-io</p>	<p>(Экспериментальная) Оптимизировать записи ввода-вывода TUN/TAP/UDP, избегая вызова в poll/epoll/select перед операцией записи. Целью такого вызова, как правило, является блокировка, пока устройство или сокет не будут готовы принять запись. Такая блокировка не является необходимой на некоторых платформах, которые не поддерживают блокировку записей на UDP-сокетах или устройствах TUN/TAP. В таких случаях можно оптимизировать петлю событий, избегая вызова в poll/epoll/select, тем самым улучшая эффективность CPU на 5-10 процентов.</p> <p>Эта опция может быть использована только в системах, отличных от Windows, когда указана опция –proto udp, и когда опция –shaper НЕ указана.</p>
<p>–multihome</p>	<p>Сконфигурировать многодомный UDP-сервер. Эта опция может быть использована, когда «OpenVPN-ГОСТ» была сконфигурирована так, чтобы слушать на всех интерфейсах, и будет пытаться привязать клиентские сеансы к интерфейсу, на который приходят пакеты, чтобы исходящие пакеты шли через этот же интерфейс. Обратите внимание, что эта опция релевантна только для UDP-серверов и в настоящее время реализована только на Linux.</p> <p>Примечание: клиенты, соединяющиеся с сервером –multihome, всегда должны использовать опцию –nobind.</p>
<p>–echo [parms...]</p>	<p>Копирует parms в вывод журнала.</p> <p>Предназначено для того, чтобы отправлять сообщения контролируемому приложению, которое получает вывод журнала «OpenVPN-ГОСТ» .</p>
<p>–remap-usr1 signal</p>	<p>Контролировать, внутренние или внешние сигналы SIGUSR1 превращаются в SIGHUP (перезапуск без сохраненного состояния) или SIGTERM (выход).</p> <p>signal может принимать значения SIGHUP или SIGTERM. По умолчанию, никакого превращения не происходит.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-verb n</p>	<p>Устанавливает подробность вывода в n (по умолчанию 1). Каждый уровень показывает всю информацию с предыдущих уровней. Уровень 3 рекомендуется, если вы хотите хороший отчет о происходящем без излишней детализации. 0 - никакого вывода, кроме фатальных ошибок. 1-3 - диапазон нормального использования. 5 - выводит символы R и W на консоль для каждого прочтенного и записанного пакета, заглавные для TCP/UDP-пакетов и строчные для TUN/TAP-пакетов. 6-11 - диапазон отладочных уровней.</p>
<p>-status file [n]</p>	<p>Записывать операционный статус в file каждые n секунд. Статус также может записываться в syslog отправлением сигнала SIGUSR2.</p>
<p>-status-version[n]</p>	<p>Выбрать номер версии формата файла статуса. Сейчас n может быть 1, 2, 3 и по умолчанию равен 1.</p>
<p>-mute n</p>	<p>Записывать в журнал не больше n последовательных сообщений одной и той же категории. Полезно для ограничения повторяющегося журналирования схожих типов сообщений.</p>
<p>-com-lzo [mode]</p>	<p>Использовать быстрое сжатие LZO - можно добавлять до 1 байта на пакет для несжимаемых данных. mode может быть «yes», «no» или «adaptive» (умолчание). В настройках серверного режима возможно избирательно включать и выключать сжатие для индивидуальных клиентов. Сначала удостоверьтесь, что конфигурационный файл клиентской стороны обеспечивает избирательное сжатие, имея по меньшей мере одну директиву -comp-lzo, такую как -comp-lzo no. Это отключит сжатие по умолчанию, но позволит будущей директиве, переданной с сервера, динамически изменять настройки включения/выключения/адаптации. Далее, в файле -client-config-dir укажите настройку сжатия для клиента, например: comp-lzo yes push «comp-lzo yes» Первая строка устанавливает настройку comp-lzo для серверной стороны соединения, вторая настраивает клиентскую сторону.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–comp-noadapt</p>	<p>При использовании вместе с –comp-lzo, эта опция отключает алгоритм адаптивного сжатия «OpenVPN-ГОСТ» . Как правило, адаптивное сжатие обеспечивается –comp-lzo.</p> <p>Адаптивное сжатие пытается оптимизировать случай, где у вас включено сжатие, но вы посылаете в основном несжимаемые (или уже сжатые) пакеты по туннелю, такие как передача по FTP или rsync большого сжатого файла. С адаптивным сжатием «OpenVPN-ГОСТ» будет периодически запускать на пробу процесс сжатия, чтобы измерить его эффективность. Если данные, передаваемые по туннелю, уже сжаты, эффективность сжатия будет очень низкой, что заставит «OpenVPN-ГОСТ» отключить сжатие на период времени до следующего пробного сжатия.</p>
<p>–management IP port [pw-file]</p>	<p>Предоставить возможность TSP-серверу на IP:port управлять функциями управления демоном. pw-file, если указано, является файлом с паролем (пароль в первой строке) или «stdin» для ввода пароля со стандартного ввода. Предоставленный пароль установит пароль, который TSP-клиенты должны будут предоставлять для доступа к функциям управления.</p> <p>Интерфейс управления также может слушать на сокете домена Unix, для тех платформ, которые это поддерживают. Чтобы использовать сокет домена Unix, укажите путь к сокету Unix вместо IP и установите значение port в «unix». В то время как умолчательное поведение - создать сокет домена Unix, с которым можно соединиться любым процессом, можно использовать директивы –management-client-user и –management-client-group, чтобы ограничить адрес.</p> <p>Интерфейс управления предоставляет специальный режим, где связь с управлением TSP может работать через сам туннель. Чтобы включить этот режим, установите значение IP в «tunnel». Туннельный режим заставит интерфейс управления слушать соединение TSP на локальном адресе VPN интерфейса TUN/TAP.</p> <p>Хотя порт управления предназначен для программного контроля других приложений над «OpenVPN-ГОСТ» , возможно связаться с портом с помощью telnet, используя клиент telnet в «грубом» режиме. Установив соединение, наберите «help», чтобы получить список команд.</p> <p>Настоятельно рекомендуется установить IP в 127.0.0.1 (localhost), чтобы ограничить доступность сервера управления для локальных клиентов.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

-management-query-passwords	Канал управления запросами для пароля закрытого ключа и логина/пароля опции -auth-user-pass. Запрашивайте через канал управления только те элементы ввода, которые, как правило, запрашиваются с консоли.
-management-forget-disconnect	Заставить «OpenVPN-ГОСТ» забывать пароли, когда сеанс управления заканчивается. Эта директива не влияет на логин и пароль опции -http-proxy. Они всегда кэшируются.
-management-hold	Запустить «OpenVPN-ГОСТ» в состоянии гибернации, пока клиент интерфейса управления не запустит ее явным образом командой hold release.
-management-signal	Послать «OpenVPN-ГОСТ» сигнал SIGUSR1, если сеанс управления обрывается. Это полезно, когда вы хотите разорвать сеанс «OpenVPN-ГОСТ» при отключении пользователя.
-management-log-cache n	Кэшировать последние n строк истории файла журнала для использования на канале управления.
-management-client-auth	Дает клиенту интерфейса управления ответственность за аутентификацию клиентов после того, как их клиентский сертификат был проверен.
-management-client-pf	Клиенты интерфейса управления должны указать файл фильтра пакетов для каждого соединяющегося клиента.
-management-client-user u	Когда интерфейс управления слушает на сокете домена Unix, позволять только соединения для пользователя u.
-management-client-group g	Когда интерфейс управления слушает на сокете домена Unix, позволять только соединения для группы g.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<code>-plugin module-pathname [init-string]</code>	<p>Загрузить подключаемый модуль из файла <code>module-pathname</code>, передавая <code>init-string</code> как аргумент в функцию инициализации модуля. В один процесс OpenVPN можно загрузить несколько подключаемых модулей.</p> <p>Несколько модулей могут быть подключены каскадом, и можно использовать модули вместе со скриптами. «OpenVPN-ГОСТ» будет вызывать модули в том порядке, в котором они декларированы в конфигурационном файле. Если для одного и того же обратного вызова сконфигурированы и модуль, и скрипт, скрипт будет вызван последним. Если код возвращения модуля/скрипта контролирует аутентификационную функцию (такую как <code>tls-verify</code>, <code>auth-user-pass-verify</code> или <code>client-connect</code>), то каждый модуль и скрипт должны вернуть успех (0), чтобы соединение было аутентифицировано.</p>
--	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.3 Серверный режим

В «OpenVPN-ГОСТ» поддерживается многоклиентный серверный режим, который может быть включен с помощью опции `-mode server`. В серверном режиме «OpenVPN-ГОСТ» слушает на одном порту входящие клиентские соединения. Все клиентские соединения маршрутизируются через один интерфейс `tun` или `tap`. Этот режим предусматривает масштабирование и должен быть в состоянии поддерживать сотни и даже тысячи клиентов на достаточно быстрых машинах. В этом режиме должна использоваться аутентификация SSL/TLS.

<code>-server network netmask</code>	<p>Вспомогательная директива, предназначенная для того, чтобы упростить конфигурацию серверного режима. Эта директива настраивает сервер «OpenVPN-ГОСТ», который присваивает клиентам адреса из указанных <code>network/netmask</code>. Сам сервер примет адрес «.1» данной сети в качестве использования как серверный конечный пункт локального интерфейса TUN/TAP. Например, <code>-server 10.8.0.0 255.255.255.0</code> расшифровывается следующим образом:</p> <pre> mode server tls-server push "topology [topology]" if dev tun AND (topology == net30 OR topology == p2p): ifconfig 10.8.0.1 10.8.0.2 if !nool: ifconfig-pool 10.8.0.4 10.8.0.251 route 10.8.0.0 255.255.255.0 if client-to-client: push "route 10.8.0.0 255.255.255.0" else if topology == net30: push "route 10.8.0.1" if dev tap OR (dev tun AND topology == subnet): ifconfig 10.8.0.1 255.255.255.0 if !nool: ifconfig-pool 10.8.0.2 10.8.0.254 255.255.255.0 push "route-gateway 10.8.0.1" </pre> <p>Не используйте опцию <code>-server</code>, если вы устанавливаете связь типа «мост». В этом случае пользуйтесь опцией <code>-server-bridge</code>.</p>
--------------------------------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<pre> -server-bridge gateway netmask pool-start-IP pool-end-IP -server-bridge ['nogw'] </pre>	<p>Вспомогательная директива, подобная <code>-server</code>, предназначенная для упрощения конфигурации «OpenVPN-ГОСТ» в серверном режиме в конфигурациях типа «мост».</p> <p>Если опция <code>-server-bridge</code> используется без каких-либо параметров, она включает режим DHCP-прокси, где подключающиеся клиенты будут получать IP-адрес для своих адаптеров TAP от DHCP-сервера, запущенного в локальной сети серверной стороны «OpenVPN-ГОСТ». Обратите внимание, что только клиенты, поддерживающие связь DHCP-клиента с адаптером TAP (такие как Windows) могут поддерживать этот режим. Опциональный флаг <code>nogw</code> указывает, что информацию о гейте не следует передавать клиенту.</p> <p>Чтобы сконфигурировать связь типа «мост», вам в первую очередь следует воспользоваться возможностями вашей операционной системы, чтобы связать «мостом» интерфейс TAP с интерфейсом NIC Ethernet. Например, в Linux это делается с помощью инструмента <code>brctl</code>, а в Windows XP это выполняется в Network Connections Panel выбором адаптеров TAP и Ethernet и щелчком правой клавишей на «Bridge Connections». Затем вы должны вручную установить IP и маску сети интерфейса «моста». Параметры <code>gateway</code> и <code>netmask</code> опции <code>-server-bridge</code> могут быть установлены или в IP и маску сети интерфейса «моста», или в IP и маску сети умолчательного гейта/роутера подсоединенной «мостом» подсети.</p> <p>Наконец, укажите диапазон IP для подсоединенной «мостом» подсети, обозначенный параметрами <code>pool-start-IP</code> и <code>pool-end-IP</code>, чтобы «OpenVPN-ГОСТ» назначала их подключающимся клиентам.</p> <p>Например, <code>server-bridge 10.8.0.4 255.255.255.0 10.8.0.128 10.8.0.254</code> расшифровывается следующим образом:</p> <pre> mode server tls-server ifconfig-pool 10.8.0.128 10.8.0.254 255.255.255.0 push "route-gateway 10.8.0.4" </pre> <p>В другом примере, <code>-server-bridge</code> (без параметров) расшифровывается как:</p> <pre> mode server tls-server push "route-gateway dhcp" </pre>
	<p>Или <code>-server-bridge nogw</code> расшифровывается как:</p> <pre> mode server tls-server </pre>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–push option</p>	<p>Передать опцию конфигурационного файла обратно клиенту для удаленного выполнения. Обратите внимание, что option должна быть окружена двойными кавычками (""). Клиент должен указать –pull в своем конфигурационном файле. Набор опций, которые могут быть переданы, ограничен как их применимостью, так и соображениями безопасности. Некоторые опции, например, выполняющие скрипты, запрещены, поскольку они в сущности позволяют скомпрометированному серверу выполнять произвольный код на клиенте. Другие опции, такие как параметры TLS и MTU, не могут быть переданы, потому что клиенту нужно знать их до того, как иницируется соединение с сервером.</p> <p>Вот частичный список опций, которые в настоящее время могут быть переданы: –route, –route-gateway, –route-delay, –redirect-gateway, –ip-win32, –dhcp-option, –inactive, –ping, –ping-exit, –ping-restart, –setenv, –persist-key, –persist-tun, –echo, –comp-lzo, –socket-flags, –sndbuf, –rcvbuf.</p>
<p>–push-reset</p>	<p>Не наследовать глобальный список переданных опций для специального экземпляра клиента. Указывайте эту опцию в клиент-специфичном контексте, например, с конфигурационным файлом –client-config-dir. Эта опция будет игнорировать опции –push на глобальном уровне конфигурационного файла.</p>
<p>disable</p>	<p>Не допустить конкретного клиента (основывается на поле common name) к соединению. Не используйте эту опцию, чтобы не допускать клиента со скомпрометированным ключом или паролем. Используйте вместо этого CRL (список отзыва сертификатов, см. опцию –crl-verify).</p> <p>Эта опция должна быть ассоциирована с конкретным экземпляром клиента, что означает, что она должна быть указана или в клиентском конфигурационном файле с использованием –client-config-dir или динамически сгенерирована с использованием скрипта –client-connect.</p>
<p>–ifconfig-pool start-IP end-IP [netmask]</p>	<p>Указать набор подсетей, динамически назначаемых соединяющимся клиентам, подобно серверу DHCP. Для туннелей в tun-стиле каждому клиенту выделяется подсеть /30 (для совместимости с клиентами Windows). Для туннелей в tap-стиле выделяются индивидуальные адреса, и необязательный параметр netmask также будет передан клиентам.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–ifconfig-pool-persist file [seconds]</p>	<p>Сохранять/удалять данные ifconfig-pool в file, через интервалы seconds (600 по умолчанию), также как и при старте и завершении работы программы.</p> <p>Цель этой опции - предоставить долгосрочную ассоциацию между клиентами (обозначенными их полями common name) и виртуальным IP-адресом, присвоенным им из ifconfig-pool. Поддержка долгосрочной ассоциации полезна для клиентов, потому что она позволяет им эффективно использовать опцию –persist-tun.</p> <p>file - ASCII-файл с разделителями-запятыми, отформатированный как <Common-Name>,<IP-address>.</p> <p>Если seconds=0, file будет рассматриваться как файл только для чтения. Это полезно, если вы хотите рассматривать file как конфигурационный файл.</p> <p>Обратите внимание, что записи в этом файле рассматриваются «OpenVPN-ГОСТ» только как предложения, основанные на прошлых ассоциациях между common name и IP-адресом. Они не гарантируют, что данное common name будет всегда получать данный IP-адрес. Если вы хотите гарантированное присвоение, пользуйтесь опцией –ifconfig-push.</p>
<p>–ifconfig-pool-linear</p>	<p>Модифицирует директиву –ifconfig-pool так, чтобы присваивать клиентам индивидуальные адреса интерфейса TUN, а не подсети /30. ПРИМЕЧАНИЕ: Эта опция несовместима с клиентами Windows.</p> <p>Эта опция не рекомендуется к использованию и должна быть заменена на опцию –topology r2r, которая функционально эквивалентна ей.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-ifconfig-push local remote-netmask</code></p>	<p>Передать виртуальные IP-конечные пункты для клиентского туннеля, заменяя динамическое присвоение <code>-ifconfig-pool</code>. Параметры <code>local</code> и <code>remote-netmask</code> устанавливаются в соответствии с директивой <code>-ifconfig</code>, которую вы хотите выполнять на клиентской машине для конфигурирования удаленного конца туннеля. Обратите внимание, что параметры <code>local</code> и <code>remote-netmask</code> существуют с точки зрения клиента, а не сервера. Они могут быть DNS-именами, а не IP-адресами, в этом случае они будут разрешаться на сервере во время соединения клиента.</p> <p>Эта опция должна быть ассоциирована с конкретным экземпляром клиента, что означает, что она должна быть указана или в конфигурационном файле экземпляра клиента с использованием <code>-client-config-file</code>, или динамически генерироваться с использованием скрипта <code>-client-connect</code>.</p> <p>Не забудьте также включить директиву <code>-route</code> в главный конфигурационный файл «OpenVPN-ГОСТ», который включает <code>local</code>, чтобы ядро знало, что его надо маршрутизировать к интерфейсу TUN/TAP сервера.</p> <p>Алгоритм выбора внутреннего клиентского IP-адреса работает следующим образом:</p> <ol style="list-style-type: none"> 1 - Используйте <code>-client-connect script</code>, сгенерированный для статического IP 2 - Используйте файл <code>-client-config dir</code> для статического IP 3 - Используйте присвоение <code>-ifconfig-pool</code> для динамического IP
---	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-iroute network [netmask]</code></p>	<p>Сгенерировать внутренний маршрут для конкретного клиента. Параметр <code>netmask</code>, если опущен, по умолчанию равен <code>255.255.255.255</code>.</p> <p>Эту директиву можно использовать, чтобы маршрутизировать фиксированную подсеть с сервера к конкретному клиенту, вне зависимости от того, откуда соединяется клиент. Помните, что вы также должны добавить маршрут к таблице маршрутизации системы (как при использовании директивой <code>route</code>). Причина, по которой нужны два маршрута, заключается в том, что директива <code>-route</code> маршрутизирует пакет из ядра в «OpenVPN-ГОСТ». Когда пакет туда попадает, директива <code>-iroute</code> маршрутизирует его к указанному клиенту.</p> <p>Эта опция должна быть указана или в конфигурационном файле клиентского экземпляра с использованием <code>-client-config-dir</code>, или в динамически сгенерированном с использованием скрипта <code>-client-connect</code>.</p> <p>Директива <code>-iroute</code> также имеет важное взаимодействие с <code>-push «route...»</code>. <code>-iroute</code> в сущности определяет подсеть, принадлежащую конкретному клиенту (назовем этого клиента А). Если вы хотите, чтобы другие клиенты могли достичь подсети А, вы должны использовать <code>-push «route...»</code> вместе с опцией <code>-client-to-client</code>, чтобы добиться этого. Чтобы все клиенты могли видеть подсеть А, «OpenVPN-ГОСТ» должна передать этот маршрут всем клиентам КРОМЕ А, поскольку подсеть уже принадлежит А. «OpenVPN-ГОСТ» достигает этого, не передавая маршрут клиенту, если он совпадает с одним из <code>iroute</code> клиента.</p>
<p><code>-client-to-client</code></p>	<p>Поскольку сервер «OpenVPN-ГОСТ» работает со множеством клиентов через один и тот же интерфейс <code>tun</code> или <code>tap</code>, он по сути является маршрутизатором. Флаг <code>-client-to-client</code> говорит «OpenVPN-ГОСТ» маршрутизировать трафик от клиента к клиенту внутри себя, а не передавать весь исходящий от клиентов трафик на интерфейс <code>TUN/TAP</code>.</p> <p>Когда используется эта опция, каждый клиент «увидит» остальных клиентов, которые в настоящее время подключены. В противном случае каждый клиент будет видеть только сервер. Не используйте эту опцию, если вы хотите фильтровать туннельный трафик через брандмауэр, используя собственные правила клиентов.</p>
<p><code>duplicate-cn</code></p>	<p>Позволить нескольким клиентам с одним и тем же <code>common name</code> одновременно подключаться. В отсутствие этой опции «OpenVPN-ГОСТ» отсоединит экземпляр клиента при подключении клиента с тем же <code>common name</code>.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–client-connect script</p>	<p>Запустить script при подключении клиента. В скрипт script передаются common name и IP-адрес только что аутентифицировавшегося клиента как переменные среды (см. раздел переменных среды ниже). В скрипт также передается путь еще не созданного временного файла как \$1 (т.е. первый аргумент командной строки), чтобы скрипт использовал его для передачи директив динамически сгенерированного конфигурационного файла в «OpenVPN-ГОСТ» .</p> <p>Если скрипт хочет генерировать динамический конфигурационный файл для использования на сервере при подключении клиента, он должен записать его в файл с именем \$1.</p> <p>См. ниже в описании опции –client-config-dir описание опций, которые могут быть правомерно использованы в динамически сгенерированном конфигурационном файле.</p> <p>Обратите внимание, что код возврата script имеет значение. Если script возвращает ненулевой ошибочный статус, клиент будет отключен.</p>
<p>–client-disconnect</p>	<p>Опция похожа на –client-connect, но вызывается при закрытии экземпляра клиента. Не будет вызвана, если для этого экземпляра не были ранее вызваны скрипт –client-connect и подключаемые модули (если определены) с успешным кодом возврата (0).</p> <p>Исключение из этого правила - если скрипт –client-disconnect или подключаемые модули подключены каскадом, и по крайней мере одна из функций опции –client-connect выполнена успешно, затем ВСЕ функции client-disconnect для скриптов и плагинов будут вызваны при удалении объекта экземпляра клиента, даже в тех случаях, когда некоторые из взаимосвязанных функций client-connect вернули ошибочный статус.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–client-config-dir dir</p>	<p>Указать каталог dir для индивидуальных клиентских конфигурационных файлов. После того, как подключающийся клиент аутентифицирован, «OpenVPN-ГОСТ» ищет в этом каталоге файл, название которого совпадает с common name клиента по правилам X.509. Если такой файл существует, он будет открыт и прочитан в поисках клиент-специфичных конфигурационных опций. Если соответствующий файл не найден, «OpenVPN-ГОСТ» попытается открыть и прочитать умолчательный файл под названием DEFAULT, который может быть предоставлен, но не обязателен.</p> <p>Этот файл может указывать фиксированный IP-адрес для данного клиента с помощью –ifconfig-push, как и фиксированные подсети, принадлежащие клиенту, с помощью –iroute.</p> <p>Одно из полезных свойств этой опции - то, что она позволяет удобно создавать, редактировать или удалять клиентские конфигурационные файлы при действующем сервере, без необходимости перезапуска сервера.</p> <p>В клиент-специфичном контексте правомочны следующие опции: –push, –push-reset, –iroute, –ifconfig-push и –config.</p>
<p>–ccd-exclusive</p>	<p>Требовать, в качестве условия аутентификации, чтобы подключающийся клиент имел файл –client-config-dir.</p>
<p>–tmp-dir dir</p>	<p>Указать каталог dir для временных файлов. Этот каталог используется скриптами –client-connect для динамической генерации клиент-специфичных конфигурационных файлов.</p>
<p>–hash-size r v</p>	<p>Установить размер таблицы хэшей реальных адресов в r, а виртуальных адресов в v. По умолчанию размеры обеих таблиц ограничены 256 адресами.</p>
<p>–bcast-buffers n</p>	<p>Назначить n буферов для широковещательных датаграмм (по умолчанию 256).</p>
<p>–tcp-queue-limit n</p>	<p>Максимальное количество исходящих пакетов, ставящихся в очередь перед TCP (по умолчанию 64).</p> <p>Когда «OpenVPN-ГОСТ» передает по туннелю данные с устройства TUN/TAP удаленному клиенту по TCP-соединению, возможно, что устройство TUN/TAP может производить данные с большей скоростью, нежели может поддерживать TCP-соединение. Когда количество исходящих пакетов, поставленных в очередь перед отправкой на TCP-сокеты, достигает этого предела для данного клиентского соединения, «OpenVPN-ГОСТ» начнет игнорировать исходящие пакеты, направленные этому клиенту.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-tcp-nodelay</p>	<p>Этот макрос устанавливает флаг сокета TCP_NODELAY на сервере и передает его соединяющимся клиентам. Флаг TCP_NODELY отключает алгоритм Нагля на TCP-сокетах, заставляя передавать пакеты немедленно с низким временем задержки, а не ждать короткий промежуток времени, чтобы объединить несколько пакетов в один большой пакет. В VPN-приложениях, работающих по TCP, TCP_NODELAY, как правило, является хорошим оптимизатором времени ожидания. Макрос расшифровывается следующим образом:</p> <pre>if mode server: socket-flags TCP_NODELAY push "socket-flags TCP_NODELAY"</pre>
<p>-max-clients n</p>	<p>Ограничить сервер n одновременно подключающимися клиентами.</p>
<p>-max-routes-per-client n</p>	<p>Позволить максимум n внутренних маршрутов на одного клиента (по умолчанию 256). Это предназначено для того, чтобы помочь сдерживать DoS-атаки, когда аутентифицированный клиент захлестывает сервер пакетами, которые, как кажется, приходят с множества уникальных MAC-адресов, заставляя сервер истощать виртуальную память по мере того, как расширяется его внутренняя таблица маршрутизации. Эту директиву можно использовать в файле -client-config-dir или автоматически генерировать скриптом -client-connect, чтобы заменить глобальное значение для конкретного клиента. Обратите внимание, что эта директива влияет на внутреннюю таблицу маршрутизации «OpenVPN-ГОСТ», а не на таблицу маршрутизации ядра.</p>
<p>-connect-freq n sec</p>	<p>Позволить максимум N новых соединений в sec секунд от клиентов. Это предназначено для того, чтобы сдерживать DoS-атаки, которые захлестывают сервер запросами на соединение, используя сертификаты, которые в конце концов не удастся аутентифицировать. Но это несовершенное решение, потому что в реальном сценарии DoS могут также быть отвергнуты правомочные соединения. Для наилучшей защиты от DoS-атак в серверном режиме используйте -proto udp и -tls-auth.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-learn-address cmd</p>	<p>Запустить скрипт или команду оболочки cmd, чтобы проверить правильность клиентских виртуальных адресов или маршрутов.</p> <p>cmd может выполняться с тремя параметрами:</p> <ol style="list-style-type: none"> 1. operation - «add», «update» или «delete», основанный на том, добавляется ли адрес к внутренней таблице маршрутизации OpenVPN, модифицируется или удаляется. 2. address - адрес узнается или не узнается. Это может быть адрес IPv4, такой как «198.162.10.14», подсеть IPv4, такая как «198.162.10.0/24», или MAC-адрес Ethernet (когда используется -dev tap) такой как «00:FF:01:02:03:04». 3. common name - Поле common name сертификата, ассоциированного с клиентом, связанным с этим адресом. Присутствует только для операций «add» и «update», но не для «delete». <p>В методах «add» и «update», если скрипт возвращает код ошибки (не ноль), «OpenVPN-ГОСТ» отвергает адрес и не модифицирует свою внутреннюю таблицу маршрутизации.</p> <p>Как правило, скрипт cmd использует информацию, предоставленную выше, чтобы установить подходящие данные брандмауэра на интерфейсе TUN/TAP. Поскольку «OpenVPN-ГОСТ» предоставляет ассоциацию между IP-адресом или MAC-адресом и аутентифицированным полем common name клиента, она позволяет определенному пользователем скрипту конфигурировать политики доступа брандмауэра с учетом высокоуровневого common name клиента, а не низкоуровневых клиентских виртуальных адресов.</p>
---------------------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–auth-user-pass-verify script method</p>	<p>Требует, чтобы клиент предоставил логин и пароль (возможно, в добавление к клиентскому сертификату) для аутентификации.</p> <p>«OpenVPN-ГОСТ» выполнит скрипт script как команду оболочки, чтобы проверить правильность логина и пароля, предоставленных клиенту.</p> <p>Если значение параметра method установлено в «via-env», «OpenVPN-ГОСТ» вызовет script с переменными среды username и password, которым в качестве значений присвоены строки логина и пароля, предоставленные клиентом. Имейте в виду, что этот способ небезопасен на некоторых платформах, которые делают среду процесса публично видимой другим непривилегированным процессам.</p> <p>Если значение параметра method установлено в «via-file», «OpenVPN-ГОСТ» запишет логин и пароль в первые две строки временного файла. Наименование файла будет передано в качестве аргумента в script, и файл будет автоматически удален «OpenVPN-ГОСТ» после того, как скрипт пришлет код завершения. Положение временного файла контролируется опцией –tmp-dir, и по умолчанию будет текущим каталогом, если не указано другое. В целях безопасности подумайте над тем, чтобы установить –tmp-dir в несохраняемую среду, такую как /dev/shm (если доступна), чтобы предотвратить запись файла с логином и паролем на жесткий диск.</p> <p>Скрипт должен просмотреть логин и пароль, возвращая успешный код (0) если запрос клиента на аутентификацию следует принять, или код ошибки (1), чтобы отказать клиенту.</p> <p>Эта директива предназначена для того, чтобы дать возможность интерфейсу в стиле подключаемых модулей расширить аутентификационные возможности «OpenVPN-ГОСТ» .</p> <p>Чтобы защититься от клиента, передающего злонамеренно созданные строки логина или пароля, логин всегда должен состоять только из следующих символов: букв алфавита и цифр, подчеркивания, дефиса, точки или at-коммерческого (@). Строка пароля может состоять из любых символов, которые можно напечатать, кроме CR и LF. Любые некорректные символы в строках логина или пароля будут превращены в знак подчеркивания.</p> <p>Все определенные пользователем скрипты должны избегать создания уязвимости защиты при работе с этими строками. Никогда не используйте эти строки так, чтобы они могли быть проинтерпретированы интерпретатором оболочки или чтобы специальные символы в них становились частью escape-последовательности.</p> <p>В качестве образца скрипта, который выполняет аутентификацию PAM, см. sample-scripts/auth-pam.pl в дистрибутиве «OpenVPN-ГОСТ» .</p>	
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–opt-verify</p>	<p>Клиенты, которые соединяются с опциями, несовместимыми с опциями сервера, будут отключены.</p> <p>Опции, которые будут сравниваться на совместимость, включают dev-type, link-mtu, tun-mtu, proto, tun-ipv6, ifconfig, comp-lzo, fragment, keydir, cipher, auth, keysize, secret, no-replay, no-iv, tls-auth, key-method, tls-server, и tls-client.</p> <p>Эта опция требует, чтобы опция –disable-oss НЕ использовалась.</p>
<p>auth-user-pass-optional</p>	<p>Позволить соединение с клиентами, которые не указывают логин и пароль. Как правило, когда указаны опции –auth-user-pass-verify или –management-client-auth (или аутентификационный подключаемый модуль), серверный демон «OpenVPN-ГОСТ» будет требовать у подключающихся клиентов указать логин и пароль. Эта опция делает передачу логина и пароля клиентами опциональной, передавая ответственность определенному пользователем аутентификационному модулю или скрипту, который будет принимать или отвергать клиента на основе других факторов (таких как набор полей сертификата X.509). Когда используется эта опция, и подключающийся клиент не передает логин и пароль, определенный пользователем аутентификационный модуль или скрипт будет рассматривать логин и пароль как пустые строки. Аутентификационный модуль или скрипт ДОЛЖЕН иметь логику, чтобы заметить это состояние и ответить соответственно.</p>
<p>client-cert-not-required</p>	<p>Не запрашивать клиентский сертификат, клиент будет аутентифицироваться только с помощью логина и пароля. Имейте в виду, что использование этой директивы менее безопасно, чем требование сертификатов со всех клиентов.</p> <p>Если вы используете эту директиву, вся ответственность за аутентификацию будет передана вашему скрипту –auth-user-pass-verify, так что имейте в виду, что ошибки в вашем скрипте могут потенциально скомпрометировать безопасность вашей VPN.</p> <p>Если вы не используете эту директиву, но указываете скрипт –auth-user-pass-verify, «OpenVPN-ГОСТ» произведет двойную аутентификацию. Потребуется успех проверки клиентского сертификата И скрипта –auth-user-pass-verify, чтобы клиент был аутентифицирован и подключен к VPN.</p>
<p>–username-as-common-name</p>	<p>Для аутентификации с помощью –auth-user-pass-verify, использовать аутентификационный логин, а не common name из клиентского сертификата в качестве common name.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–no-name-remapping</p>	<p>Позволить строкам Common Name, X509 Subject и логина включать любой печатный символ, включая пробел, но исключая контрольные символы, такие как табуляция, новая строка и возврат каретки.</p> <p>По умолчанию «OpenVPN-ГОСТ» преобразует любой символ, отличный от букв и цифр, подчеркивания, дефиса, точки и косой черты в подчеркивание. Строка X509 Subject, возвращенная переменной среды tls_id, может дополнительно содержать двоеточие или знак равенства.</p> <p>Хотя преобразование имен выполняется в целях безопасности, чтобы уменьшить вероятность введения строки, создающей уязвимость, в определенных пользователем аутентификационных скриптах, эта опция предоставляется для тех случаев, где желательно отключить преобразование. Используйте эту опцию только в том случае, если вы знаете, что делаете!</p>
<p>–port-share host port</p>	<p>При работе в TCP-серверном режиме, использовать порт OpenVPN совместно с другим приложением, таким как HTTPS-сервер. Если «OpenVPN-ГОСТ» почувствует соединение на своем порту, которое использует протокол, отличный от протокола OpenVPN, она проксирует соединение к серверу на host:port. В настоящее время работает только с HTTP/HTTPS, хотя теоретически ее в будущем возможно расширить на другие протоколы, такие как ssh.</p> <p>Не реализована в Windows.</p>

8.4 Клиентский режим

Используйте клиентский режим, подключаясь к серверу «OpenVPN-ГОСТ», который имеет в конфигурации опции –server, –server-bridge или –mode server.

<p>–client</p>	<p>Вспомогательная директива, предназначенная для того, чтобы упростить конфигурацию клиентского режима «OpenVPN-ГОСТ». Эта директива эквивалентна следующему:</p> <pre>pull tls-client</pre>
----------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-pull</p>	<p>Эта опция должна применяться на клиенте, соединяющемся с многоклиентным сервером. Она указывает, что «OpenVPN-ГОСТ» должна принять опции, переданные сервером, если они являются частью правомочного набора передаваемых опций (обратите внимание, что опция -pull подразумевается опцией -client).</p> <p>В частности, -pull позволяет серверу передавать клиенту маршруты, так что не следует использовать -pull и -client в ситуациях, когда вы не доверяете серверу контроль над таблицей маршрутизации клиента.</p>
<p>-auth-user-pass [up]</p>	<p>Аутентифицироваться на сервере с помощью логина и пароля. up - файл, содержащий логин и пароль в 2 строках (примечание: «OpenVPN-ГОСТ» будет читать пароли только из файла, созданного с помощью конфигурационной опции -enable-password-save, или в Windows с помощью определения ENABLE_PASSWORD_SAVE в config-win32.h.)</p> <p>Если параметр up опущен, логин и пароль будут запрашиваться с консоли.</p> <p>Серверная конфигурация должна указать скрипт -auth-user-pass-verify, чтобы проверить логин и пароль, предоставленные клиентом.</p>
<p>-auth-retry type</p>	<p>Контролировать, как «OpenVPN-ГОСТ» отвечает на ошибки проверки логина и пароля, такие как ответ с клиентской стороны на сообщение сервера AUTH_FAILED или неудача проверки пароля закрытого ключа.</p> <p>Как правило, используется, чтобы предотвратить аутентификационные ошибки от фатальности на клиентской стороне, и позволить перезапросить логин и пароль в случае ошибки.</p> <p>Сообщение AUTH_FAILED генерируется сервером, если клиент не проходит аутентификацию -auth-user-pass, или если серверный скрипт -client-connect возвращает статус ошибки, когда клиент пытается подключиться.</p> <p>type может быть одним из:</p> <p>none - Клиент выходит с фатальной ошибкой (умолчание)</p> <p>pointinteract - Клиент попытается переподключиться без перезапроса логина и пароля -auth-user-pass. Используйте эту опцию для необслуживаемых клиентов.</p> <p>interact - У клиента будет перезапрошен логин и пароль и/или пароль закрытого ключа перед попыткой переподключения.</p> <p>Обратите внимание, что хотя эта опция не может быть передана, ей можно управлять с интерфейса управления.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–server-poll-timeout n</p>	<p>Циклически опрашивая возможные удаленные сервера, чтобы подключиться, тратить не больше n секунд на ожидание ответа, прежде чем перейти к следующему серверу.</p>
<p>–explicit-exit-notify [n]</p>	<p>В UDP-клиентском режиме или в режиме точка-в-точку посылать серверу/партнеру сообщение о выходе, если туннель перезапускается или процесс OpenVPN завершается. В клиентском режиме, при выходе/перезапуске, эта опция сообщит серверу, что следует немедленно закрыть его объект экземпляра клиента, а не ждать таймаута. Параметр n (по умолчанию 1) управляет максимальным количеством попыток, которые предпримет клиент, посылая сообщение о выходе.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.5 Опции зашифрования канала данных

Эти опции имеют значение и для статического режима, и для режима TLS-договоренного ключа (должны быть совместимы между партнерами)

<p><code>-secret file [direction]</code></p>	<p>Обеспечить режим зашифрования статического ключа (не TLS). Использовать ранее полученный обоими партнерами секретный ключ <code>file</code>, который был сгенерирован с помощью опции <code>-genkey</code>.</p> <p>Опциональный параметр <code>direction</code> обеспечивает использование 4 различных ключей (HMAC-отправка, шифр-зашифрование, HMAC-получение, шифр-расшифрование), так что каждое направление течения данных имеет различный набор ключей HMAC и зашифования. Это имеет ряд желательных защитных свойств, включая исключение определенных видов DoS-атак и атак перепроигрывания сообщений.</p> <p>Когда параметр <code>direction</code> опущен, 2 ключа используются в двух направлениях, один для HMAC и один для зашифрования/расшифрования.</p> <p>Параметр <code>direction</code> всегда должен иметь дополняющие друг друга значения на обеих сторонах соединения, т.е. одна сторона должна использовать «1», а другая использовать «0», или обе стороны должны его опустить полностью.</p> <p>Параметр <code>direction</code> требует, чтобы файл <code>file</code> содержал 2048-битный ключ.</p> <p>Режим зашифровки на статическом ключе имеет определенные преимущества, наиболее важное из которых - легкость конфигурирования.</p> <p>Нет сертификатов, удостоверяющих центров или сложных договорных хэндшейков и протоколов. Единственное требование - чтобы у вас был ранее существующий защищенный канал с вашим партнером (такой как <code>ssh</code>), чтобы изначально скопировать ключ. Это требование, вместе с фактом, что ваш ключ никогда не меняется, если вы не сгенерируете вручную новый, делает этот режим несколько менее безопасным, чем режим TLS (см. ниже). Если атакующему удастся украсть ваш ключ, все, что было когда-либо зашифровано им, скомпрометировано. Сравните это с идеальными возможностями секретности в TLS-режиме (с использованием обмена ключами Диффи-Хеллмана), где даже если атакующему удалось украсть ваш закрытый ключ, он не получит никакой информации, которая помогла бы ему расшифровать предыдущие сеансы.</p>
--	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>Еще один преимущественный аспект режима зашифрования со статическим ключом тот, что это протокол, в котором отсутствуют хэндшейки, нет никаких отличительных подписей или признаков (таких как заголовок последовательности хэндшейка протокола) которые отмечали бы зашифрованные пакеты как сгенерированные «OpenVPN-ГОСТ» . Любой, подслушивающий на проводе, не увидит ничего, кроме случайно выглядящих данных.</p>
<p>–auth alg</p>	<p>Аутентифицировать пакеты с HMAC, используя алгоритм дайджеста alg. (По умолчанию SHA1). HMAC - часто используемый алгоритм аутентификации сообщений (MAC), использующий строку данных, безопасный алгоритм хэширования и ключ для создания цифровой подписи.</p> <p>«OpenVPN-ГОСТ» использует HMAC, чтобы сначала зашифровать пакет, потом обработать HMAC получившийся зашифрованный текст.</p> <p>В режиме шифрования со статическим ключом, ключ HMAC включен в ключевой файл, сгенерированный опцией –genkey. В режиме TLS ключ HMAC генерируется динамически и передается партнерам через контрольный канал TLS. Если «OpenVPN-ГОСТ» получает пакет с плохим HMAC, она отбрасывает этот пакет. HMAC обычно добавляет от 16 до 20 байтов на пакет. Чтобы отключить аутентификацию, установите значение параметра alg в none.</p>
<p>–cipher alg</p>	<p>Шифровать пакеты с помощью алгоритма шифрования alg. По умолчанию BF-CBC, сокращение от режима Blowfish in Cipher Block Chaining. Этот режим имеет следующие преимущества: он быстр, очень надежен и допускает размеры ключей до 448 битов. Данный режим предназначен для использования в ситуациях, когда ключи меняются нечасто.</p> <p>Чтобы увидеть, какие еще шифры доступны в «OpenVPN-ГОСТ» , используйте опцию –show-ciphers.</p> <p>«OpenVPN-ГОСТ» поддерживает режимы шифрования CBC, CFB и OFB, однако CBC рекомендуется, а CFB и OFB должны считаться дополнительными режимами.</p> <p>Установите значение параметра alg в none, чтобы отключить шифрование.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–keysize n</p>	<p>Размер ключа шифрования в битах (опционально). Если не указана, по умолчанию равна умолчательному значению, специфичному для данного шифра. Опция –show-chipers (см. ниже) показывает все доступные шифры OpenSSL, их умолчательные размеры ключей, и можно ли изменить размер ключа. Меняйте умолчательный размер ключа с осторожностью. Многие шифры не были широко криптоанализированы с нестандартными длинами ключей, и более длинный ключ может не предоставлять реальной гарантии большей безопасности и даже уменьшить степень защиты.</p>
<p>–prng alg [nsl]</p>	<p>(Дополнительная) для PRNG (генератора псевдослучайных чисел) использовать алгоритм дайджеста alg (по умолчанию sha1) и установить nsl (по умолчанию 16) в размер в байтах длины секрета поппе (между 16 и 64). Установите значение параметра alg в поппе, чтобы отключить PRGN и использовать вместо нее функцию OpenSSL RAND_bytes для всех требований псевдослучайных чисел в «OpenVPN-ГОСТ» .</p>
<p>–engine [engine-name]</p>	<p>Обеспечить функциональность криптографического модуля engine OpenSSL, основанную на аппаратных возможностях. Если указан параметр engine-name, использовать определенный криптографический модуль engine. Используйте опцию –show-engines, чтобы получить список криптографических модулей engine, которые поддерживаются OpenSSL.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–no-replay</p>	<p>(Дополнительная) Отключить защиту «OpenVPN-ГОСТ» против атак перепроигрывания. Не используйте эту опцию, если вы не готовы заплатить уменьшением степени защиты за увеличение эффективности.</p> <p>«OpenVPN-ГОСТ» предоставляет защиту от перепроигрывания датаграмм по умолчанию.</p> <p>Защита от перепроигрывания выполняется помечанием каждой исходящей датаграммы идентификатором, который гарантированно уникален для используемого ключа. Партнер, который получает датаграмму, проверяет уникальность идентификатора. Если этот идентификатор уже был получен в предыдущей датаграмме, «OpenVPN-ГОСТ» проигнорирует пакет.</p> <p>Защита от перепроигрывания важна для того, чтобы отразить такие атаки, как атака переполнения SYN, где атакующий слушает на проводе, перехватывает пакет SYN (идентифицируя его по контексту, в котором он встречается по отношению к другим пакетам), потом передает получающему партнеру множество копий этого пакета.</p> <p>Защита от перепроигрывания в «OpenVPN-ГОСТ» реализована несколько различными способами, в зависимости от режима управления ключами, который вы выбрали.</p> <p>В режиме статического ключа или при использовании шифров СFB или OFB, «OpenVPN-ГОСТ» использует 64-битный уникальный идентификатор, который сочетает метку времени с увеличивающимися последовательными номерами.</p> <p>При использовании режима TLS для обмена ключами и шифра СВС, «OpenVPN-ГОСТ» использует только 32-битный последовательный номер без метки времени, поскольку «OpenVPN-ГОСТ» может гарантировать уникальность этой величины для каждого ключа. Как в IPSec, если последовательный номер приближается к нулю, «OpenVPN-ГОСТ» запускает новый обмен ключами.</p> <p>Чтобы производить проверку на перепроигрывание, «OpenVPN-ГОСТ» использует алгоритм «скользящего окна», используемый IPSec.</p>
-------------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–replay-window n [t]</p>	<p>Использовать скользящее окно для защиты от перепроигрывания размера n и временное окно в t секунд.</p> <p>По умолчанию n равно 64 (умолчание IPSec), а t равно 16 секундам.</p> <p>Эта опция актуальна только в режиме UDP, т.е. когда или указана опция –proto udp, или вообще не указана опция –proto.</p> <p>Когда OpenVPN туннелирует IP-пакеты через UDP, существует возможность, что пакеты могут быть потеряны или доставлены в неправильном порядке. Поскольку «OpenVPN-ГОСТ», как и IPSec, эмулирует слой физической сети, она примет последовательность пакетов, пришедших в неправильном порядке, и доставит такие пакеты в том же порядке, в каком они были получены, в стек протоколов TCP/IP, если они удовлетворяют некоторым ограничениям.</p> <ol style="list-style-type: none"> 1. Пакет не может быть перепроигрыванием (если только не указана опция –no-replay, которая отключает защиту от перепроигрывания) 2. Если пакет прибывает в неправильном порядке, он может быть принят только если разница между его последовательным номером и самым большим уже принятым последовательным номером меньше n. 3. Если пакет прибывает в неправильном порядке, он будет принят только если он прибывает не позже чем t секунд после любого пакета, содержащего более высокий последовательный номер. <p>Если вы используете сетевую связь с большой магистралью (что означает широкую полосу пропускания и большой период ожидания), вы можете захотеть использовать большие величины n. Особенно часто этого требует спутниковая связь.</p> <p>Если вы запускаете «OpenVPN-ГОСТ» с –verb 4, вы увидите сообщение «Replay-window backtrack occurred [x]» каждый раз, когда отступление максимального последовательного номера увеличивается. Это может быть использовано для калибровки n.</p> <p>Существуют некоторые противоречия по поводу подходящего способа обращения с изменением порядка пакетов в слое безопасности.</p> <p>А именно, до какой степени должен слой безопасности защищать инкапсулированный протокол от атак, которые приносятся разновидностями обычной потери и перестановки пакетов, которые случаются в IP-сетях?</p> <p>Подход IPSec и «OpenVPN-ГОСТ» состоит в том, чтобы разрешить перестановку пакетов внутри определенного фиксированного окна последовательных номеров.</p>
-----------------------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>«OpenVPN-ГОСТ» дополняет модель IPSec, ограничивая размер окна во времени, как и в пространстве последовательности.</p> <p>«OpenVPN-ГОСТ» также добавляет TCP-транспорт как опцию (не предлагаемую IPSec), в этом случае «OpenVPN-ГОСТ» может занять очень строгую позицию по отношению к удалению и перестановке сообщений: не позволять этого. Поскольку TCP гарантирует надежность, любая потеря или перестановка пакетов может быть сочтена атакой.</p> <p>В этом смысле можно возразить, что туннельный TCP-транспорт предпочтителен при туннелировании не-IP или UDP-протоколов приложений, которые могут быть уязвимы по отношению к атаке удаления или перестановки пакетов, которая не удастся в пределах нормальных операционных параметров IP-сетей.</p> <p>Поэтому утверждается, что никогда не следует туннелировать не-IP-протокол или UDP-протокол приложения через UDP, если протокол может быть уязвим по отношению к атаке удаления или перестановки пакетов, которая не удастся в пределах нормальных операционных параметров того, что следует ожидать от физического IP-слоя. Проблема легко решается простым использованием TCP в качестве транспортного слоя VPN.</p>
<p>-mute-replay-warnings</p>	<p>Не выводить предупреждения о перепроигрывании, которые часто бывают ложной тревогой в WiFi-сетях. Эта опция сохраняет безопасность кода защиты от перепроигрывания без вывода множества сообщений о дублирующихся пакетах.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-replay-persist file</p>	<p>Сохранять состояние защиты от перепроигрывания между сеансами, используя файл file для сохранения и перезагрузки состояния.</p> <p>Эта опция усиливает защиту против атак перепроигрывания, особенно когда вы используете «OpenVPN-ГОСТ» в динамическом контексте (например, с опцией -ineta), когда сеансы «OpenVPN-ГОСТ» часто начинаются и останавливаются.</p> <p>Эта опция сохранит на диске копию текущего состояния защиты от перепроигрывания (т.е. самую последнюю метку времени пакета и последовательный номер, полученные от удаленного партнера), так что если сеанс «OpenVPN-ГОСТ» остановлен и начат снова, он отвергнет любое переигрывание пакетов, которые были уже получены в предыдущей сессии.</p> <p>Эта опция имеет смысл только в том случае, когда защита от перепроигрывания включена (по умолчанию) и вы используете или -secret (режим общих секретных ключей) или TLS-режим с -tls-auth.</p>
<p>-no-iv</p>	<p>(Дополнительная) Отключить использование IV (вектора инициализации шифра). Не используйте эту опцию, если вы не готовы заплатить меньшей степенью защиты за большую эффективность.</p> <p>«OpenVPN-ГОСТ» использует IV по умолчанию и требует его для режимов CFB и OFB (которые совершенно не защищены без него). Использование IV важно для безопасности, когда несколько сообщений зашифровываются/расшифровываются с использованием одного и того же ключа.</p> <p>IV реализован по-разному в зависимости от используемого режима шифрования.</p> <p>В режиме CBC, «OpenVPN-ГОСТ» использует псевдослучайный IV для каждого пакета.</p> <p>В режиме CFB/OFB «OpenVPN-ГОСТ» использует в качестве IV уникальный последовательный номер и метку времени. На самом деле, в режиме CFB/OFB «OpenVPN-ГОСТ» использует оптимизацию датаграмм, экономящую место, которая использует уникальный идентификатор для защиты от перепроигрывания датаграмм в качестве IV.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–test-crypto</p>	<p>Выполнить самотестирование криптографических опций «OpenVPN-ГОСТ», зашифровывая и расшифровывая тестовые пакеты с использованием опций зашифрования каналов данных, указанных выше. Эта опция не требует функционирующего партнера, поэтому может быть указана без –dev и –remote.</p> <p>Типичным использованием –test-crypto будет что-то подобное следующему:</p> <pre>openvpn –test-crypto –secret key</pre> <p>или</p> <pre>openvpn –test-crypto –secret key –verb 9</pre> <p>Эта опция очень полезна для тестирования «OpenVPN-ГОСТ» после того, как она была портирована на новую платформу, или чтобы изолировать проблемы в компиляторе, криптобиблиотеке OpenSSL или криптографическом коде «OpenVPN-ГОСТ». Поскольку это режим самотестирования, проблемы с зашифрованием и аутентификацией могут быть решены независимо от проблем с сетью и туннелем.</p>
---------------------	---

8.6 Опции режима TLS

Режим TLS - самый мощный криптографический режим «OpenVPN-ГОСТ» как в области безопасности, так и в области гибкости. Режим TLS работает путем установления контрольных туннелей и туннелей данных, которые мультиплексированы через один TCP/UDP-порт. «OpenVPN-ГОСТ» инициирует TLS-сеанс по контрольному каналу и использует его, чтобы произвести обмен ключами шифрования и HMAC для защиты канала данных. Режим TLS использует развитый слой криптостойкости над UDP-соединением для всех коммуникаций по контрольному каналу, в то время как канал данных, через который проходят зашифрованные туннельные данные, форвардится без какого-либо посредничества. Результат наилучший в обоих мирах: быстрый канал данных, который форвардится через UDP с непроизводительными издержками только в виде функций зашифрования, расшифрования и HMAC, и контрольный канал, который предоставляет все возможности защиты TLS, включая аутентификацию, основанную на сертификатах, и секретность форвардинга Диффи-Хеллмана.

Чтобы использовать режим TLS, каждый партнер, который запускает «OpenVPN-ГОСТ», должен иметь собственную локальную пару сертификат/ключ (–cert и –key), подписанную на корневом сертификате, указанном в –sa.

Когда два партнера подключаются друг к другу, каждый представляет другому свой локальный сертификат. Затем каждый партнер проверяет, что его партнер предоставил сертификат, подписанный на корневом сертификате, указанном в –sa.

Если эта проверка успешна для обоих партнеров, то будет успешно установлено TLS-соединение, оба партнера обменяются временными сеансовыми ключами, и туннель начнет передавать данные.

Дистрибутив «OpenVPN-ГОСТ» содержит набор скриптов для управления RSA-сертификатами и ключами, размещенными в поддиректории easy-rsa.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-tls-server</p>	<p>Включить TLS и принять на себя роль сервера во время хэндшейка. Обратите внимание, что «OpenVPN-ГОСТ» разработана как приложение, работающее в режиме от-партнера-к-партнеру. Определение клиента или сервера существует только в целях установления контрольного канала TLS.</p>
<p>-tls-client</p>	<p>Включить TLS и принять на себя роль клиента во время хэндшейка.</p>
<p>-ca file</p>	<p>Файл удостоверяющего центра (CA) в формате .pem, также именуемый корневым сертификатом. Этот файл может включать несколько сертификатов в формате .pem, конкатенированных вместе. Вы можете сконструировать свой собственный сертификат и закрытый ключ удостоверяющего центра, используя такую команду, как:</p> <pre>openssl req -days 3650 -nodes -new -newkey gost2001:A -x509 -keyout ca.key -out ca.crt</pre> <p>Затем отредактируйте ваш файл openssl.cnf и отредактируйте переменную certificate так, чтобы она указывала на ваш новый корневой сертификат ca.crt.</p> <p>Только для тестовых целей, дистрибутив «OpenVPN-ГОСТ» включает образец сертификата удостоверяющего центра (ca.crt). Конечно, вам никогда не следует использовать тестовые сертификаты и тестовые ключи из дистрибутива «OpenVPN-ГОСТ» в рабочей обстановке, поскольку вследствие того факта, что они включены в дистрибутив «OpenVPN-ГОСТ», они не предоставляют никакой защиты.</p>
<p>-dh file</p>	<p>Файл, содержащий параметры Диффи-Хеллмана в формате .pem (требуется только для -tls-server). Используйте команду <code>openssl dhparam -out dh1024.pem 1024</code> для генерации вашего собственного файла, или используйте существующий файл dh1024.pem, включенный в дистрибутив «OpenVPN-ГОСТ». Параметры Диффи-Хеллмана могут считаться открытыми.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–cert file</p>	<p>Подписанный сертификат локального партнера в формате .pem - должен быть подписан удостоверяющим центром, чей сертификат находится в файле –ca file. Каждый партнер в «OpenVPN-ГОСТ», работающей в режиме TLS, должен иметь свои собственные файлы сертификата и закрытого ключа. В дополнение, каждый сертификат должен быть подписан ключом удостоверяющего центра, чей открытый ключ находится в файле удостоверяющего центра –ca. Вы легко можете создать свой собственный удостоверяющий центр (см. выше) или заплатить деньги, чтобы использовать коммерческий сервис. Чтобы создать сертификат, вы можете использовать такую команду, как:</p> <pre>openssl req -days 3650 -nodes -new -newkey gost2001:A -keyout server.key -out server.csr -extensions tlsserver</pre> <p>или</p> <pre>openssl req -days 3650 -nodes -new -newkey gost2001:A -keyout client.key -out client.csr -extensions tlsclient</pre> <p>Если закрытый ключ вашего удостоверяющего центра живет на другой машине, скопируйте запрос на подпись сертификата (mycert.csr) на эту другую машину (это можно сделать по незащищенному каналу, например, по электронной почте). Теперь подпишите сертификат такой командой, как</p> <pre>openssl ca -batch -days 3650 -out server.crt -in server.csr -md md_gost94 -extensions tlsserver</pre> <p>или</p> <pre>openssl ca -batch -days 3650 -out client.crt -in client.csr -md md_gost94 -extensions tlsclient</pre> <p>Теперь скопируйте сертификат (mycert.crt) обратно к партнеру, который изначально создал файл .csr (это можно сделать через публичную среду). Обратите внимание, что команда openssl ca читает местоположение ключа удостоверяющего центра из своего конфигурационного файла, такого как /usr/share/ssl/openssl.cnf - также обратите внимание, что для функций удостоверяющего центра вы должны создать файлы index.txt (может быть пустым) и serial (инициализируйте, установив 01).</p>
<p>–key file</p>	<p>Закрытый ключ локального партнера в формате .pem. Используйте закрытый ключ, который был создан, когда вы создавали ваш партнерский сертификат (см. выше опцию –cert file).</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–pkcs12 file</p>	<p>Указать файл формата PKCS#12, содержащий локальный закрытый ключ, локальный сертификат и корневой сертификат УЦ. Эту опцию можно использовать вместо –ca, –cert и –key.</p>
<p>–pkcs11-cert-private [0 1]...</p>	<p>Установить, если доступ к объекту сертификата должен быть выполнен после логина. У каждого провайдера собственные настройки.</p>
<p>–pkcs11-id name</p>	<p>Указать сериализованный сертификат, который следует использовать. id должен быть получен независимой опцией – show-pkcs11-ids.</p>
<p>–pkcs11-id-management</p>	<p>Получить id PKCS#11 с интерфейса управления. В этом случае сообщение NEED-STR 'pkcs11-id-request' будет инициализировано в реальном времени, приложение может использовать команду pkcs11-id-count, чтобы получить доступное количество сертификатов, и команду pkcs11-id-get, чтобы получить id и тело сертификата.</p>
<p>–pkcs11-pin-cache seconds</p>	<p>Указать, сколько секунд можно кэшировать PIN. По умолчанию - пока токен не удален.</p>
<p>–pkcs11-protectd-authentication [0 1]...</p>	<p>Использовать защищенный путь аутентификации PKCS#11, полезный для биометрических устройств и внешних клавиатур. У каждого провайдера свои собственные настройки.</p>
<p>–pkcs11-providers provider...</p>	<p>Указать провайдеров RSA Security Inc. PKCS#11 Cryptographic Token Interface (Cryptoki), которых следует загрузить. Эту опцию можно использовать вместо –cert, –key и –pkcs12.</p>
<p>–pkcs11-private-mode mode</p>	<p>Указать, какой способ использовать для выполнения операций с закрытым ключом. Можно указать собственный режим для каждого провайдера. Режим кодируется как шестнадцатеричное число и может быть одной из следующих масок: 0 (умолчание) - попытаться определить автоматически. 1- использовать подпись. 2 - использовать восстановление подписи. 4 - использовать расшифрование. 8 - использовать разворачивание.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–cryptoapicert select-string</p>	<p>Загрузить сертификат и закрытый ключ из системного хранилища сертификатов Windows (только в Windows). Используйте эту опцию вместо –cert и –key. Это делает возможным использовать любые смарткарты, поддерживаемые Windows, а также любой вид сертификата, находящегося в хранилище сертификатов, если у вас есть доступ к соответствующему закрытому ключу. Эта опция тестировалась с парой различных смарт-карт (GemSAFE, Cryptoflex и Swedish Post Office eID) на клиентской стороне, а также импортированный программный PKCS#12-сертификат на серверной стороне. Чтобы выбрать сертификат на основе поиска по подстроке в поле subject сертификата: <code>cryptoapicert "SUBJ:Peter Runestig"</code> Чтобы выбрать сертификат на основе отпечатка сертификата: <code>cryptoapicert "THUMB:f6 49 24 41 01 b4 ..."</code> Шестнадцатеричную строку отпечатка можно легко копировать из графического интерфейса хранилища сертификатов Windows.</p>
-------------------------------------	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–key-method m</p>	<p>Использовать метод согласования ключей канала данных m. Ключевой метод должен совпадать на обеих сторонах соединения.</p> <p>После того, как «OpenVPN-ГОСТ» согласует сеанс TLS, генерируется новый набор ключей для защиты канала туннельных данных, и производится обмен ключами через сеанс TLS.</p> <p>В методе 1 обе стороны создают случайные ключи зашифрования и HMAC-отправки, которые форвардятся на другой хост по каналу TLS.</p> <p>В методе 2 (умолчание) клиент генерирует случайный ключ. Кроме того, и клиент, и сервер генерируют какое-то количество случайного инициализационного материала. Весь материал источника ключей обменивается через канал TLS. Настоящие ключи создаются с помощью функции TLS PRF, которая берет энтропию источника и с клиента, и с сервера.</p> <p>Обратите внимание, что в режиме TLS встречаются два уровня ключевания:</p> <ol style="list-style-type: none"> 1. Соединение TLS изначально согласовывается, обе стороны соединения предоставляют сертификаты и проверяя сертификат (или другую аутентификационную информацию) другой стороны. Параметр –key-method не оказывает никакого влияния на этот процесс. 2. После того, как соединение TLS установлено, туннельные сеансовые ключи отдельно согласуются по существующему защищенному TLS-каналу. Здесь –key-method определяет происхождение туннельных сеансовых ключей.
<p>–tls-cipher l</p>	<p>Список l разрешенных TLS-шифров, разделенных двоеточиями. Если вы требуете высокий уровень защиты, вы, возможно, захотите установить этот параметр вручную, чтобы предотвратить атаку отката версий, где человек посередине пытается заставить двух партнеров договариваться на самом низком уровне защиты, который они оба поддерживают. Используйте опцию –show-tls, чтобы увидеть список поддерживаемых TLS-шифров.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–tls-timeout n</p>	<p>Установить таймаут повторной передачи пакетов на контрольном канале TLS, если никакого отзыва от удаленного партнера не приходит в течение n секунд (по умолчанию n=2). Когда «OpenVPN-ГОСТ» отправляет контрольный пакет своему партнеру, она ожидает получение отзыва в течение n секунд, она еще раз передаст пакет в соответствии с ТСП-подобным алгоритмом экспоненциального возврата. Этот параметр применяется только к пакетам контрольного канала. На пакеты канала данных (которые несут зашифрованные туннельные данные) никогда не приходит отзыв, и они никогда не передаются повторно, потому что сетевые протоколы более высокого уровня, работающие на вершине туннеля, такие как ТСП, ожидают, что эта роль оставлена им.</p>
<p>–reneg-bytes n</p>	<p>Пересогласовать ключ канала данных после того, как n байтов отправлены или получены (по умолчанию отключено). «OpenVPN-ГОСТ» позволяет выразить срок жизни ключа как количество зашифрованных/расшифрованных байтов, количество пакетов или секунд. Пересогласование ключа будет произведено насильно, если любой из партнеров соответствует любому из этих трех критериев.</p>
<p>–reneg-pkts n</p>	<p>Пересогласовать ключ канала данных после того, как n пакетов отправлены и получены (по умолчанию отключено).</p>
<p>–reneg-sec n</p>	<p>Пересогласовать ключ канала данных после n секунд (по умолчанию 3600). При использовании двухфакторной аутентификации обратите внимание, что эта умолчательная величина может привести к тому, что конечного пользователя будут принуждать переаутентифицироваться раз в час. Также помните, что эта опция может быть использована и на клиенте, и на сервере, и пересогласование запустит тот из партнеров, у кого указана меньшая величина. Частая ошибка - установить –reneg-sec в большую величину на клиенте или на сервере, в то время как другая сторона по-прежнему использует умолчательную величину в 3600 секунд, что значит, что пересогласование по-прежнему будет происходить каждые 3600 секунд. Решение состоит в том, чтобы увеличить величину –reneg-sec и на клиенте, и на сервере, или установить ее в 0 на одной из сторон соединения (чтобы отключить), и в выбранную величину на другой стороне.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–hand-window n</p>	<p>Окно хэндшейка - основанный на TLS обмен ключами должен завершиться в течение n секунд после инициации хэндшейка любым из партнеров (по умолчанию 60 секунд). Если хэндшейк не завершается успешно, мы попытаемся переустановить наше соединение с нашим партнером и попытаемся снова. Даже в случае провала хэндшейка мы будем использовать наш завершающий время действия ключ до –tran-window секунд, чтобы поддержать непрерывность передачи туннельных данных.</p>
<p>tran-window n</p>	<p>Окно передачи - наш старый ключ может жить столько секунд после того, как начинается новое пересогласование ключа (по умолчанию 3600 секунд). Эта возможность позволяет корректно перейти от старого ключа к новому и удаляет последовательность пересогласования ключа с критичного пути форвардинга туннельных данных.</p>
<p>–single-session</p>	<p>После исходного соединения с удаленным партнером, запретить все новые соединения. Использование этой опции означает, что удаленный партнер не может подключиться, отключиться и снова подключиться.</p> <p>Если демон перегружается от сигнала или опции –ping-restart, он позволит одно новое соединение.</p> <p>Опцию –single-session можно использовать с опциями –ping-exit или –inactive, чтобы создать один динамический сеанс, который отключится по завершении.</p>
<p>–tls-exit</p>	<p>Отключиться, если согласование TLS не удастся.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-tls-auth-file [direction]</code></p>	<p>Добавить дополнительный слой аутентификации HMAC на верх контрольного канала TLS для защиты от DoS-атак.</p> <p>В двух словах, <code>-tls-auth</code> подключает своего рода «брандмауэр HMAC» на TCP/UDP-порту «OpenVPN-ГОСТ», где пакеты контрольного канала TLS, несущие некорректную подпись HMAC, могут быть немедленно проигнорированы без ответа. Параметр <code>file</code> (необходим) - ключевой файл, который может быть в одном из двух форматов.</p> <ol style="list-style-type: none"> 1. Файл статического ключа «OpenVPN-ГОСТ», созданный опцией <code>-genkey</code> (необходим, если используется параметр <code>direction</code>). 2. Файл парольной фразы в свободной форме. В этом случае ключ HMAC получается при взятии безопасного хэша этого файла, подобно командам <code>md5sum</code> и <code>shasum</code>. <p>«OpenVPN-ГОСТ» сначала пробует формат (1), и если файл не удастся прочесть как файл статического ключа, будет использоваться формат (2).</p> <p>См. в опции <code>-secret</code> информацию об опциональном параметре <code>direction</code>.</p> <p>Опция <code>-tls-auth</code> рекомендуется, когда вы запускаете «OpenVPN-ГОСТ» в режиме, в котором она слушает пакеты с любого IP-адреса, например когда опция <code>-remote</code> не указана или указана с <code>-float</code>.</p> <p>Обоснование этой опции таково. TLS требует многопакетного обмена, прежде чем она сможет аутентифицировать партнера. В течение этого времени перед аутентификацией «OpenVPN-ГОСТ» назначает ресурсы (память и CPU) этому потенциальному партнеру. Потенциальный партнер также открывает много частей «OpenVPN-ГОСТ» и библиотеки OpenSSL пакетам, которые он посылает. Сегодня наиболее удачные сетевые атаки пытаются либо использовать ошибки в программах (такие как атаки переполнения буфера) или вынудить программу поглотить столько ресурсов, что ее становится невозможно использовать. Конечно, первая линия защиты - всегда предоставлять чистый, хорошо просмотренный код. «OpenVPN-ГОСТ» была написана с предотвращением атак переполнения буфера в качестве первого приоритета. Но как показала история, многие из наиболее широко используемых сетевых приложений время от времени падали жертвами атак переполнения буфера.</p> <p>Поэтому в качестве второй линии защиты «OpenVPN-ГОСТ» предлагает этот специальный слой аутентификации на верху контрольного канала TLS, так чтобы каждый пакет в контрольном канале аутентифицировался подписью HMAC и уникальным ID для защиты от атак перепроигрывания.</p>
--	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>Эта подпись также должна помочь защититься от DoS-атак (атак отказа в обслуживании). Важным ключевым правилом в уменьшении уязвимости к DoS-атакам является минимизировать количество ресурсов, которые может потребить потенциальный, но еще не аутентифицированный клиент.</p> <p>Опция <code>-tls-auth</code> делает это, подписывая каждый пакет контрольного канала TLS подписью HMAC, включая пакеты, которые отправляются до того, как уровень TLS имел шанс аутентифицировать партнера. Результат таков, что пакеты без корректной подписи могут быть проигнорированы сразу после получения, прежде чем у них будет шанс поглотить дополнительные системные ресурсы, такие как инициализация TLS-хэндшейка. Опция <code>-tls-auth</code> может быть усилена добавлением опции <code>-replay-persist</code>, которая сохранит статус защиты «OpenVPN-ГОСТ» от атак перепроигрывания в файл, чтобы он не терялся при перезапусках.</p> <p>Следует подчеркнуть, что эта возможность опциональна и что файл пассфразы/ключа, используемый с опцией <code>-tls-auth</code>, не дает партнеру ничего, кроме возможности инициализировать хэндшейк TLS. Он не используется для зашифрования или аутентификации каких-либо туннельных данных.</p>
<p><code>-askpass [file]</code></p>	<p>Получить пароль к сертификату с консоли или из файла <code>[file]</code>, прежде чем мы демонизируемся.</p> <p>Для особенно надежной защиты можно защитить ваш закрытый ключ паролем. Конечно, это означает, что каждый раз, когда демон «OpenVPN-ГОСТ» запускается, вы должны быть там, чтобы ввести пароль. Опция <code>-askpass</code> позволяет вам запускать «OpenVPN-ГОСТ» из командной строки. Она запросит у вас пароль, прежде чем демонируется. Чтобы защитить закрытый ключ паролем, вы должны опустить опцию <code>-nodes</code>, когда пользуетесь командно-строчным инструментом <code>openssl</code> для управления сертификатами и закрытыми ключами.</p> <p>Если указан файл <code>file</code>, читать пароль из первой строки этого файла. Помните, что хранение вашего пароля в файле до определенной степени понижает дополнительную защиту, которую предоставляет использование зашифрованного ключа. (Примечание: «OpenVPN-ГОСТ» будет читать пароли из файла только в том случае, если она была собрана с конфигурационной опцией <code>-enable-password-save</code>, или в Windows с определением <code>ENABLE_PASSWORD_SAVE</code> в файле <code>config-win32.h</code>).</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–auth-nocache</p>	<p>Не кэшировать логины и пароли опции –askpass или –auth-user-pass в виртуальной памяти.</p> <p>Если эта директива указана, она заставит «OpenVPN-ГОСТ» немедленно забыть вводы логина и пароля, как только они использованы. В результате, когда «OpenVPN-ГОСТ» нужны логин и пароль, она запросит их ввод со стандартного ввода, что может произойти несколько раз за время сеанса OpenVPN.</p> <p>Эта директива не влияет на логин и пароль опции –http-проху. Он всегда кэшируется.</p>
<p>–tls-verify cmd</p>	<p>Выполнить команду оболочки cmd, чтобы проверить имя X509 name текущего TLS-соединения, которое уже прошло все остальные сертификационные тесты (кроме отзыва через директиву –crl-verify; тест на отзыв производится после теста –tls-verify).</p> <p>cmd должна вернуть 0, чтобы позволить TLS-хэндшейку продолжаться, или 1 в случае неудачи. cmd выполняется как:</p> <pre>cmd certificate_depth X509_NAME_oneline</pre> <p>Эта возможность полезна, если партнер, которому вы хотите доверять, имеет сертификат, который был подписан удостоверяющим центром, который также подписал много других сертификатов, если вы не хотите доверять им всем, а предпочитаете избирательно относиться к тому, какой сертификат партнера вы примете. Эта функциональность позволяет вам написать скрипт, который будет проверять имя X509 name сертификата и решит, следует его принимать или нет. В качестве простого скрипта на perl, который проверяет поле common name сертификата, см. файл verify-sp в дистрибутиве «OpenVPN-ГОСТ» .</p> <p>См. в разделе «Переменные среды» ниже информацию о дополнительных параметрах, передаваемых как переменные среды.</p> <p>Обратите внимание, что команда cmd может быть командой оболочки с несколькими аргументами, в этом случае все аргументы, созданные «OpenVPN-ГОСТ» , будут добавлены в конец строки cmd, чтобы создать строку, которая будет передана в скрипт.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p><code>-tls-remote name</code></p>	<p>Принимать соединения только от хоста с именем X509 <code>name</code> или <code>common name</code>, совпадающим с <code>name</code>. Удаленный хост также должен пройти все аутентификационные тесты.</p> <p>Примечание: поскольку <code>tls-удаленный хост</code> может тестироваться на префикс поля <code>common name</code>, используйте эту опцию только когда вы пользуетесь «OpenVPN-ГОСТ» со специально созданным сертификатом, находящимся под вашим контролем. Никогда не используйте эту опцию, когда ваши клиентские сертификаты подписаны кем-то третьими, например, коммерческим сетевым УЦ.</p> <p><code>Name</code> также может быть префиксом поля <code>common name</code>, например, если вы хотите, чтобы клиент принимал соединения только с «Server-1», «Server-2» и т.д., вы можете просто воспользоваться опцией вида <code>-tls-remote Server</code>.</p> <p>Использование префикса поля <code>common name</code> - полезная альтернатива управлению CRL (списка отзыва сертификатов) на клиенте, поскольку она позволяет клиенту отвергнуть все сертификаты, кроме ассоциированных с указанными серверами.</p> <p>Опция <code>-tls-remote</code> - полезная замена опции <code>-tls-verify</code> для проверки удаленного хоста, потому что <code>-tls-remote</code> работает и в окружении <code>-chroot</code>.</p>
<p><code>-ns-cert-type client server</code></p>	<p>Потребовать, чтобы сертификат партнера был подписан явно заданным определением <code>nsCertType</code> «client» или «server».</p> <p>Это полезная защитная опция для клиентов, обеспечивающая тот факт, что хост, с которым они соединяются, определенно является сервером.</p> <p>См. скрипт <code>easy-rsa/build-key-server</code> в качестве примера, как создать сертификат с полем <code>nsCertType</code>, установленным в значение «server».</p> <p>Если поле <code>nsCertType</code> серверного сертификата установлено в значение «server», клиенты могут проверить это с помощью опции <code>-ns-cert-type server</code>.</p> <p>Это важная предосторожность для защиты против атаки «человек посередине», где авторизованный клиент пытается соединиться с другим клиентом, притворяясь сервером. Атака легко предотвращается, если клиенты проверяют серверный сертификат с использованием одной из опций <code>-ns-cert-type</code>, <code>-tls-remote</code> или <code>-tls-verify</code>.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-remote-cert-ku v...</p>	<p>Потребовать, чтобы сертификат партнера был подписан явно заданным key usage. Это полезная защитная опция для клиентов, обеспечивающая тот факт, что хост, с которым они соединяются, определенно является сервером. key usage следует закодировать в шестнадцатеричное число, можно указать более одного key usage.</p>
<p>-remote-cert-eku oid</p>	<p>Потребовать, чтобы сертификат партнера был подписан явно заданным extended key usage. Это полезная защитная опция для клиентов, обеспечивающая тот факт, что хост, с которым они соединяются, определенно является сервером. extended key usage следует закодировать в нотации OID или символическом представлении OpenSSL.</p>
<p>-remote-cert-tls client server</p>	<p>Потребовать, чтобы сертификат партнера был подписан явно заданными key usage и explicit key usage, основанными на правилах TLS, приведенных в RFC3280. Это полезная защитная опция для клиентов, обеспечивающая тот факт, что хост, с которым они соединяются, определенно является сервером. Опция -remote-cert-tls client эквивалентна -remote-cert-ku 80 08 88 -remote-cert-eku «TLS Web Client Authentication». Key usage - digitalSignature и/или keyAgreement. Опция -remote-cert-tls server эквивалентна -remote-cert-ku a0 88 -remote-cert-eku «TLS Web Server Authentication». Key usage - digitalSignature и (keyEnchpherment или keyAgreement). Это важная предосторожность для защиты против атаки «человек посередине», где авторизованный клиент пытается соединиться с другим клиентом, притворяясь сервером. Атака легко предотвращается, если клиенты проверяют серверный сертификат с использованием одной из опций -remote-cert-tls, -tls-remote или -tls-verify.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>-crl-verify crl</p>	<p>Проверить, не указан ли сертификат партнера в файле crl в формате PEM. CRL (список отзыва сертификатов) используется, когда конкретный ключ скомпрометирован, но вся PKI сохранена. Предположим, что у вас была PKI, состоящая из УЦ, корневого сертификата и нескольких клиентских сертификатов. Предположим, что ноутбук, содержащий ключ и сертификат клиента, был украден. Добавив украденный сертификат в файл CRL, вы можете отвергнуть любое соединение, которое попытается им воспользоваться, сохраняя общую целостность PKI. Единственный случай, когда необходимо пересоздавать всю PKI заново - если был скомпрометирован сам корневой сертификат.</p>
------------------------	--

8.7 Информация по библиотеке SSL

<p>-show-ciphers</p>	<p>(Независимая) Показать все алгоритмы шифров, которые можно использовать с опцией -cipher</p>
<p>-show-digests</p>	<p>(Независимая) Показать все алгоритмы дайджестов, которые можно использовать с опцией -auth</p>
<p>-show-tls</p>	<p>(Независимая) Показать все шифры TLS (где TLS используется только как контрольный канал). Шифры TLS будут отсортированы от самого высокого предпочтения (самый безопасный) к самому низкому.</p>
<p>-show-engines</p>	<p>(Независимая) Показать доступные в настоящее время основанные на аппаратном оборудовании модули engine криптографической акселерации, поддерживаемые библиотекой OpenSSL.</p>

8.8 Создание случайного ключа

Эти опции используются только для режима зашифрования со статическим ключом, не для TLS.

<p>-genkey</p>	<p>(Независимая) Создать случайный ключ для использования в качестве общего секрета с опцией -secret. Этот файл должен быть передан партнеру по ранее существовавшему защищенному каналу, такому как scp.</p>
<p>-secret file</p>	<p>Записать ключ в файл file.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.9 Режим конфигурации сохраняемого туннеля TUN/TAP

Доступен на Linux 2.4.7+. Эти опции включают в себя независимый режим «OpenVPN-ГОСТ», который может быть использован для создания и удаления сохраняемых туннелей.

<p><code>-mktun</code></p>	<p>(Независимая) Создать сохраняемый туннель на платформах, которые поддерживают их, таких, как Linux. Как правило, туннели TUN/TAP существуют только в течение того периода времени, когда приложение держит их открытыми. Эта опция пользуется способностью драйвера TUN/TAP создавать сохраняемые туннели, которые сохраняются в течение нескольких запусков «OpenVPN-ГОСТ» и закрываются только когда их удаляют или когда машина перезагружается.</p> <p>Одно из преимуществ сохраняемых туннелей - то, что они исключают необходимость для отдельных скриптов <code>-up</code> и <code>-down</code> запускать соответствующие команды <code>ifconfig</code> и <code>route</code>. Эти команды могут быть помещены в тот же скрипт оболочки, который начинает или заканчивает сеанс «OpenVPN-ГОСТ».</p> <p>Еще одно преимущество в том, что открытые соединения через туннель, основанный на TUN/TAP, не будут перезагружены, если партнер по «OpenVPN-ГОСТ» перезапускается. Это может быть полезным, чтобы предоставить непрерывную связь через туннель в случае DHCP-перезагрузки открытого IP-адреса партнера (см. опцию <code>-ipchange</code> выше).</p> <p>Один недостаток сохраняемых туннелей состоит в том, что труднее автоматически конфигурировать их величину MTU (см. опции <code>-link-mtu</code> и <code>-tun-mtu</code> выше).</p> <p>На некоторых платформах, таких как Windows, туннели TAP-Win32 сохраняются по умолчанию.</p>
<p><code>-rmtun</code></p>	<p>(Независимая) Удалить сохраняемый туннель</p>
<p><code>-dev tunX tapX</code></p>	<p>Устройство TUN/TAP</p>
<p><code>-user user</code></p>	<p>Опциональный пользователь, который должен быть владельцем этого туннеля</p>
<p><code>-group group</code></p>	<p>Опциональная группа, которая должна быть владельцем этого туннеля.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.10 Опции, специфичные для Windows

<p><code>-win-sys path 'env'</code></p>	<p>Установить путь к системному каталогу Windows для использования при поиске системных выполняемых файлов, таких как <code>route.exe</code> и <code>netsh.exe</code>. По умолчанию, если эта директива не указана, путь устанавливается в <code>C:\WINDOWS</code>. Специальная строка <code>'env'</code> указывает, что путь следует считать с переменной среды <code>SystemRoot</code>.</p>
<p><code>-ip-win32 method</code></p>	<p>Используя опцию <code>-ifconfig</code> в Windows, установить адрес и сетевую маску адаптера TAP-Win32 с использованием <code>method</code>. Не используйте эту опцию, если вы также используете <code>-ifconfig</code>.</p> <p><code>manual</code> - Не устанавливать IP-адрес или сетевую маску автоматически. Вместо этого вывести сообщение на консоль, требующее от пользователя сконфигурировать адаптер вручную и указывающее IP/сетевую маску, которые «OpenVPN-ГОСТ» ожидает в качестве установок адаптера.</p> <p><code>dynamic [offset] [lease-time]</code> - Автоматически установить IP-адрес и сетевую маску, отвечая на DHCP-запросы, созданные ядром. Этот режим - вероятно, «самое чистое» решение для установки свойств TCP/IP, поскольку он использует хорошо известный протокол DHCP. Но существуют два предварительных требования для использования этого режима.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>1. Свойства TCP/IP для адаптера TAP-Win32 должны быть установлены в «Obtain an IP address automatically»</p> <p>2. «OpenVPN-ГОСТ» необходимо потребовать IP-адрес в подсети для использования в качестве адреса виртуального сервера DHCP. По умолчанию в режиме -dev tap «OpenVPN-ГОСТ» возьмет, как правило, неиспользуемый первый адрес в подсети. Например, если ваша подсеть 192.168.4.0, а сетевая маска 255.255.255.0, то «OpenVPN-ГОСТ» возьмет IP-адрес 192.168.4.0 в качестве адреса виртуального сервера DHCP. В режиме -dev tun «OpenVPN-ГОСТ» заставит сервер DHCP вести себя так, будто он установлен в удаленном конечном пункте.</p> <p>Опциональный параметр offset - целое число между -256 и 256, по умолчанию равное 0. Если offset больше 0, сервер DHCP будет вести себя как IP-адрес при сетевом адресе + offset. Если offset меньше 0, DHCP будет вести себя как IP-адрес при широковещательном адресе + offset. Можно использовать команду Windows ipconfig /all, чтобы показать, чем Windows считает адрес сервера DHCP. «OpenVPN-ГОСТ» «потребует» этот адрес, поэтому обязательно используйте свободный адрес. Тем не менее, различные экземпляры «OpenVPN-ГОСТ», включая различные концы одного и того же соединения, могут использовать один и тот же адрес виртуального сервера DHCP. Параметр lease-time контролирует время аренды присваивания DHCP, данного адаптеру TAP-Win32, и выражается в секундах. Как правило, предпочтительно очень большое время аренды, потому что оно предотвращает потерю маршрутов, включающих адаптер TAP-Win32, когда система засыпает. Умолчательное время аренды - один год.</p> <p>netsh - автоматически установить IP-адрес и маску сети, используя командно-строчную команду Windows «netsh». Этот способ, похоже, корректно работает на Windows XP, но не на Windows 2000.</p> <p>ipapi - автоматически установить IP-адрес и маску сети, используя Windows IP Helper API. Этот подход не имеет идеальной семантики, хотя тестирование показало, что на практике он работает хорошо. Если вы используете эту опцию, лучше всего оставить свойства TCP/IP для адаптера TAP-Win32 в умолчательном состоянии, т.е. «Obtain an IP address automatically».</p>
--	---

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

	<p>adaptive - (Умолчание) изначально попытаться использовать способ dynamic, затем перейти к netsh, если согласование DHCP с адаптером TAP-Win32 не завершается успешно за 20 секунд. Такие случаи известны, когда пакеты некоего стороннего брандмауэра, установленного на клиентской машине, блокируют согласование DHCP, используемое адаптером TAP-Win32. Обратите внимание, что если происходит переход к netsh, TCP/IP-свойства адаптера TAP-Win32 будут переустановлены с DHCP на статические, и это заставит будущие перезапуски «OpenVPN-ГОСТ», использующей режим adaptive, сразу же использовать netsh, не используя сначала dynamic. Чтобы «переключить» режим adaptive с использования netsh, запустите «OpenVPN-ГОСТ» по крайней мере один раз с использованием режима dynamic, чтобы восстановить TCP/IP-свойства адаптера TAP-Win32 в конфигурацию DHCP.</p>
<p>-route-method m</p>	<p>Какой способ m использовать для добавления маршрутов в Windows?</p> <p>adaptive (умолчание) - сначала попытаться использовать IP helper API. Если это не удастся, вернуться к команде оболочки route.exe.</p> <p>ipapi - использовать IP helper API.</p> <p>exe - вызвать команду оболочки route.exe.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–dhcp-option type [parm]</p>	<p>Установить расширенные TCP/IP-свойства адаптера TAP-Win32, опция должна использоваться с –ip-win32 dynamic или –ip-win32 adaptive. Эту опцию можно использовать, чтобы установить дополнительные TCP/IP-свойства адаптера TAP-Win32, и особенно полезна для конфигурирования клиента OpenVPN для достижения сервера Samba через VPN.</p> <p>DOMAIN name - установить DNS-суффикс, специфичный для соответствующего соединения.</p> <p>DNS addr - установить адрес первичного сервера доменных имен. Повторить эту опцию, чтобы установить адреса вторичных DNS-серверов.</p> <p>WINS addr - Установить адрес первичного WINS-сервера (NetBIOS over TCP/IP Name Server). Повторить эту опцию, чтобы установить адреса вторичных WINS-серверов.</p> <p>NBDD addr - Установить адрес первичного NBDD-сервера (NetBIOS over TCP/IP Datagram Distribution Server). Повторить эту опцию, чтобы установить адреса вторичных NBDD-серверов.</p> <p>NTP addr - установить адрес первичного NTP-сервера (Network Time Protocol). Повторить эту опцию, чтобы установить адреса вторичных NTP-серверов.</p> <p>NBT type - установить тип узла NetBIOS over TCP/IP. Возможные опции: 1 - b-узел (широковещание), 2 - p-узел (именные запросы точка-в-точку к WINS-серверу), 4 - m-узел (широковещание, затем сервер имен запросов) и 8 - h-узел (сервер имен запросов, затем широковещание).</p> <p>NBS scope-id - установить область действия NetBIOS over TCP/IP. ID области действия NetBIOS предоставляет расширенный сервис имен для модуля NetBIOS over TCP/IP (известного как NBT). Главная цель ID области действия NetBIOS - изолировать трафик NetBIOS в одной сети так, чтобы он проходил только через узлы с тем же ID области действия NetBIOS. ID области действия NetBIOS - символьная строка, которая добавляется к имени NetBIOS. ID области действия NetBIOS на двух хостах должен совпадать, или два хоста не смогут общаться. ID области действия NetBIOS также позволяет компьютерам использовать одно и то же компьютерное имя, потому что у них разные ID области действия. ID области действия становится частью имени NetBIOS, делая это имя уникальным.</p> <p>DISABLE-NBT - отключить NetBIOS-over-TCP/IP.</p> <p>Обратите внимание, что если опция –dhcp-option передана через –push клиенту, работающему не в Windows, опция будет сохранена в окружении клиента перед тем, как будет вызван скрипт up, под названием «foreign_option_n».</p>
---------------------------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–tap-sleep n</p>	<p>Заставить «OpenVPN-ГОСТ» заснуть на n секунд сразу же после того, как состояние адаптера TAP-Win32 установлено в «connected».</p> <p>Эта опция предназначена для использования при проблемах с опциями –ifconfig и –ip-win32, и используется, чтобы дать адаптеру TAP-Win32 время подняться, прежде чем к нему будут применены операции Windows IP Helper API.</p>
<p>–show-net-up</p>	<p>Вывести взгляд «OpenVPN-ГОСТ» на системную таблицу маршрутизации и список сетевых адаптеров в syslog или файл журнала после того, как был поднят адаптер TUN/TAP и были добавлены какие-либо маршруты.</p>
<p>–dhcp-renew</p>	<p>Попросить Windows обновить аренду адаптера TAP при запуске. Эта опция, как правило, не является необходимой, потому что Windows автоматически запускает пересогласование DHCP на адаптере TAP, когда он поднимается, однако если вы установили свойство Media Status адаптера TAP-Win32 в «Always Connected», вам может понадобиться этот флаг.</p>
<p>–dhcp-release</p>	<p>Попросить Windows освободить аренду адаптера TAP при выключении. Эта опция имеет те же оговорки, что и –dhcp-renew.</p>
<p>–register-dns</p>	<p>Запустить net stop dnscache, net start dnscache, ipconfig /flushdns и ipconfig /registerdns при инициации соединения. Известно, что это заставляет Windows узнавать переданные DNS-серверы.</p>
<p>–pause-exit</p>	<p>Вывести сообщение «press any key to continue» на консоль, прежде чем программа «OpenVPN-ГОСТ» завершает работу. Эта опция автоматически используется проводником Windows, когда «OpenVPN-ГОСТ» запущена с конфигурационным файлом, выбранным с помощью контекстного меню проводника.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

<p>–service exit-event [0 1]</p>	<p>Следует использовать, когда «OpenVPN-ГОСТ» автоматически запускается другой программой в таком контексте, что никакое взаимодействие с пользователем через монитор или клавиатуру невозможно. В общем, конечным пользователям не следует иметь необходимость явным образом использовать эту опцию, потому что она автоматически добавляется сервисной оболочкой «OpenVPN-ГОСТ», когда данная конфигурация «OpenVPN-ГОСТ» запускается как сервис.</p> <p>exit-event - имя объекта глобального события Windows, и «OpenVPN-ГОСТ» будет непрерывно проверять состояние этого объекта события и завершит работу, когда объект станет сигнализированным.</p> <p>Второй параметр указывает исходное состояние параметра exit-event и, как правило, по умолчанию равен 0.</p> <p>Может выполняться одновременно несколько процессов «OpenVPN-ГОСТ» с одним и тем же параметром exit-event. В любом случае контролирующий процесс может сигнализировать exit-event, заставляя все такие процессы завершиться. При выполнении процесса «OpenVPN-ГОСТ» с директивой –service, у «OpenVPN-ГОСТ», вероятно, не будет консольного окна для вывода сообщений о статусе и ошибках, поэтому полезно использовать опции –log или –log-append, чтобы записывать эти сообщения в файл.</p>
<p>–show-adapters</p>	<p>(Независимая) Показать доступные адаптеры TAP-Win32, которые могут быть выбраны с помощью опции –dev-node. В системах, отличных от Windows, команда ifconfig предоставляет сходную функциональность.</p>
<p>–allow-nonadmin [TAP-adapter]</p>	<p>(Независимая) Установить TAP-адаптер так, чтобы позволить доступ от не-администраторов. Если параметр TAP-adapter опущен, все TAP-адаптеры системы будут сконфигурированы так, чтобы позволить неадминистративный доступ. Настройка неадминистративного доступа будет продолжаться только тот период времени, пока объект устройства TAP-Win32 и драйвер остаются загруженными, и ее необходимо будет снова устанавливать после перезагрузки, или если драйвер был выгружен и снова загружен. Эту директиву может использовать только администратор.</p>

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

-show-valid-subnets	(Независимая) Показать действительные подсети для эмуляции -dev tun. Поскольку драйвер TAP-Win32 экспортирует интерфейс ethernet в Windows, и поскольку устройства TUN по своей природе работают точка-в-точку, для драйвера TAP-Win32 необходимо накладывать некоторые ограничения на выбор адресов в конечном пункте TUN. А именно, конечные пункты точка-в-точку, использованные в эмуляции устройства TUN, должны быть два адреса из середины подсети /30 (сетевая маска 255.255.255.252).
-show-net	(Независимая) Показать взгляд «OpenVPN-ГОСТ» на системную таблицу маршрутизации и список сетевых адаптеров.

8.11 Независимые опции PKCS#11

-show-pkcs11-ids provider [cert_private]	(Независимая) Показать список объектов токенов PKCS#11. Установить [cert_private] в 1, если сертификаты хранятся как частные объекты. Опция -verb может быть использована ДО этой опции, чтобы предоставить отладочную информацию.
--	---

8.12 Скриптование и переменные среды

«OpenVPN-ГОСТ» экспортирует ряд переменных среды, использующихся в скриптах, определенных пользователем.

8.12.1 Порядок выполнения скриптов

-up	Выполняется после того, как связывается сокет TCP/UDP и открывается TUN/TAP.
-tls-verify	Выполняется, когда у нас есть пока еще недоверенный удаленный партнер.
-ipchange	Выполняется после аутентификации соединения или изменения удаленного IP-адреса.
-client-connect	Выполняется в режиме -mode server сразу после клиентской аутентификации.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

-route-up	Выполняется после аутентификации соединения, или сразу же, или спустя несколько секунд, время ожидания определяется опцией -route-delay.
-client-disconnect	Выполняется в режиме -mode server при закрытии экземпляра клиента.
-down	Выполняется после закрытия TCP/UDP и TUN/TAP.
-learn-address	Выполняется в режиме -mode-server, когда или адрес/маршрут IPv4 или адрес MAC добавляется во внутреннюю таблицу маршрутизации «OpenVPN-ГОСТ» .
-auth-user-pass-verify	Выполняется в режиме -mode-server при подключении новых клиентов, когда клиент еще не является доверенным.

8.12.2 Типы и преобразование строк

В определенных случаях «OpenVPN-ГОСТ» выполняет преобразование символов в строках. А именно, любые символы, не входящие в набор разрешенных символов для каждого типа строк, будут преобразованы в знак подчеркивания.

Вопрос. Почему преобразование строк необходимо?

Ответ. Это важная защитная функция, предназначенная для того, чтобы предотвратить злонамеренное кодирование строк из недоверенных источников, которые передаются как параметры в скрипты, сохраняются в среде, используются в качестве common name, переводятся в имя файла и т.д.

Вопрос. Можно ли отключить преобразование строк?

Ответ. Да, используя опцию -no-name-mapping, однако эту опцию следует считать дополнительной.

Вот краткое описание имеющихся в «OpenVPN-ГОСТ» типов строк и разрешенных классов символов для каждой строки.

Имена, составленные по правилам X.509: буквы и цифры, знак подчеркивания (_), дефис (-), точка (.), at-коммерческое (@), двоеточие (:), косая черта (/) и знак равенства (=). Буквы и цифры определяются как символы, которые заставляют функцию библиотеки C isalnum() вернуть значение «истинно».

Поля Common Name: Буквы и цифры, знак подчеркивания (_), дефис (-), точка (.) и at-коммерческое (@).

-auth-user-pass username: То же, что у полей Common Name, с одним исключением: параметр username передается в плагин OPENVPN_PLUGIN_AUTH_USER_PASS_VERIFY как есть, без преобразования.

-auth-user-pass password: Любой «печатный» символ, кроме CR и LF. Печатные символы определяются как символы, которые заставляют функцию библиотеки C isprint() вернуть значение «истинно».

-client-config-dir filename как производные от полей common name или username: Буквы и цифры, знак подчеркивания (_), дефис (-) и точка (.), за исключением «.» и «.» в качестве отдельных строк, а также символ at-коммерческое (@), добавленный для совместимости

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

с классом символов `common name`.

Имена переменных среды: буквы и цифры или знак подчеркивания (`_`).

Значения переменных среды: любой печатный символ.

Во всех случаях, символы в строке, которые не являются членами разрешенного класса символов для этого типа строк, преобразовываются в знак подчеркивания.

8.12.3 Переменные среды

Однажды установленная переменная среды сохраняется, пока ее не переустановят или не будет перезапущена система.

В серверном режиме переменные среды, установленные «OpenVPN-ГОСТ», определяются в соответствии с объектами клиентов, с которыми они ассоциированы, поэтому не должно быть случаев, когда скрипты получают доступ к ранее установленным переменным, которые относятся к другим экземплярам клиентов.

<code>bytes_received</code>	Общее количество байтов, полученных от клиента во время сеанса VPN. Устанавливается перед выполнением скрипта <code>-client-disconnect</code> .
<code>bytes_sent</code>	Общее количество байтов, переданных клиенту во время сеанса VPN. Устанавливается перед выполнением скрипта <code>-client-disconnect</code> .
<code>common_name</code>	Поле <code>common name</code> аутентифицированного клиента. Устанавливается перед выполнением скриптов <code>-client-connect</code> , <code>-client-disconnect</code> и <code>-auth-user-pass-verify</code> .
<code>config</code>	Имя первого файла <code>-config</code> . Устанавливается при инициации программы и переустанавливается при <code>SIGUP</code> .
<code>daemon</code>	Устанавливается в «1», если указана директива <code>-daemon</code> , и в «0» во всех остальных случаях. Устанавливается при инициации программы и переустанавливается при <code>SIGUP</code> .
<code>daemon_log_redirect</code>	Устанавливается в «1», если определены директивы <code>log</code> или <code>log-append</code> , и в «0» во всех остальных случаях. Устанавливается при инициации программы и переустанавливается при <code>SIGUP</code> .
<code>dev</code>	Действительное имя устройства TUN/TAP, включая номер, если он существует. Устанавливается перед выполнением скриптов <code>-up</code> или <code>-down</code> .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

foreign_option_n	Опция, переданная директивой <code>-push</code> клиенту, который не обладает встроенной поддержкой этой опции, например, опция <code>-dhcp-option</code> в системе, отличной от Windows, будет записана в эту последовательность переменных среды перед выполнением скрипта <code>-up</code> .
ifconfig_broadcast	Широковещательный адрес для сегмента виртуальной сети ethernet, определяемый из опции <code>-ifconfig</code> при использовании опции <code>-dev tap</code> . Устанавливается перед тем, как «OpenVPN-ГОСТ» вызывает команду <code>ifconfig</code> или <code>netsh</code> (версия <code>ifconfig</code> для Windows), что обычно случается до выполнения скрипта <code>-up</code> .
ifconfig_local	IP-адрес локального конечного пункта VPN, указанный в опции <code>-ifconfig</code> (первый параметр). Устанавливается перед тем, как «OpenVPN-ГОСТ» вызывает команду <code>ifconfig</code> или <code>netsh</code> (версия <code>ifconfig</code> для Windows), что обычно случается до выполнения скрипта <code>-up</code> .
ifconfig_remote	IP-адрес удаленного конечного пункта VPN, указанный в опции <code>-ifconfig</code> (второй параметр) при использовании опции <code>-dev tun</code> . Устанавливается перед тем, как «OpenVPN-ГОСТ» вызывает команду <code>ifconfig</code> или <code>netsh</code> (версия <code>ifconfig</code> для Windows), что обычно случается до выполнения скрипта <code>-up</code> .
ifconfig_netmask	Маска подсети сегмента виртуальной сети ethernet, указанная как второй параметр опции <code>-ifconfig</code> при использовании опции <code>-dev tap</code> . Устанавливается перед тем, как «OpenVPN-ГОСТ» вызывает команду <code>ifconfig</code> или <code>netsh</code> (версия <code>ifconfig</code> для Windows), что обычно случается до выполнения скрипта <code>-up</code> .
ifconfig_pool_local_ip	Локальный виртуальный IP-адрес для туннеля TUN/TAP, взятый из директивы <code>-ifconfig-push</code> , если она указана, или же из диапазона <code>ifconfig</code> (который управляется директивой конфигурационного файла <code>-ifconfig pool</code>). Устанавливается только для туннелей с опцией <code>-dev tun</code> . Эта опция устанавливается на сервере перед выполнением скриптов <code>-client-connect</code> и <code>-client-disconnect</code> .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

ifconfig_pool_netmask	Сетевая маска виртуального IP для туннеля TUN/TAP, взятая из директивы <code>-ifconfig-push</code> , если она указана, или же из файла <code>ifconfig pool</code> (который управляется директивой конфигурационного файла <code>-ifconfig pool</code>). Устанавливается только для туннелей с опцией <code>-dev tap</code> . Эта опция устанавливается на сервере прежде выполнением скриптов <code>-client-connect</code> и <code>-client-disconnect</code> .
ifconfig_pool_remote_ip	Удаленный виртуальный IP-адрес для туннеля TUN/TAP, взятый из директивы <code>-ifconfig-push</code> , если она указана, или же из файла <code>ifconfig pool</code> (который управляется директивой конфигурационного файла <code>-ifconfig pool</code>). Эта опция устанавливается на сервере перед выполнением скриптов <code>-client-connect</code> и <code>-client-disconnect</code> .
link_mtu	Максимальный размер пакета (без учета IP-заголовка) туннельных данных в режиме транспорта в UDP-туннеле. Устанавливается перед выполнением скриптов <code>-up</code> и <code>-down</code> .
local	Параметр опции <code>-local</code> . Устанавливается при запуске программы и переустанавливается при SIGNUP.
local_port	Номер локального порта, указанный опцией <code>-port</code> или <code>-lport</code> . Устанавливается при запуске программы и переустанавливается при SIGNUP.
password	Пароль, предоставленный подключающимся клиентом. Устанавливается перед выполнением скрипта <code>-auth-user-pass-verify</code> , только когда указан модификатор <code>via-env</code> , и удаляется из среды после того, как скрипт возвращает значение.
proto	Параметр опции <code>-proto</code> . Устанавливается при запуске программы и переустанавливается при SIGNUP.
remote_n	Параметр опции <code>-remote</code> . Устанавливается при запуске программы и переустанавливается при SIGNUP.
remote_port_n	Номер удаленного порта, указанный опцией <code>-port</code> или <code>-rport</code> . Устанавливается при запуске программы и переустанавливается при SIGNUP.
route_net_gateway	Ранее существовавший умолчательный IP-гейт в таблице маршрутизации системы. Устанавливается перед выполнением скрипта <code>-up</code> .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

route_vpn_gateway	Умолчательный гейт, используемый опциями <code>-route</code> , указанный либо в опции <code>-route-gateway</code> либо в качестве второго параметра опции <code>-ifconfig</code> , когда указана опция <code>-dev tun</code> . Устанавливается перед выполнением скрипта <code>-up</code> .
route_parm_n	Набор переменных, которые определяют каждый добавляемый маршрут, и устанавливаются перед выполнением скрипта <code>-up</code> . parm может иметь значения «network», «netmask», «gateway» или «metric». n - номер маршрута «OpenVPN-ГОСТ», начиная с 1. Если сеть или гейт являются разрешимыми именами DNS, будут записываться трансляции их IP-адресов вместо их имен, как указано в командной строке или конфигурационном файле.
script_context	Устанавливается в «init» или «restart» перед выполнением скрипта <code>up/down</code> . Дополнительную информацию см. в описании опции <code>-up</code> .
script_type	Один из следующих скриптов: <code>up</code> , <code>down</code> , <code>ipchange</code> , <code>route-up</code> , <code>tls-verify</code> , <code>auth-user-pass-verify</code> , <code>client-connect</code> , <code>client-disconnect</code> , или <code>learn-address</code> . Устанавливается перед выполнением любого скрипта.
signal	Причина выхода или перезагрузки. Может быть одним из <code>sigusr1</code> , <code>sighup</code> , <code>sigterm</code> , <code>sigint</code> , <code>inactive</code> (управляемым опцией <code>-inactive</code>), <code>ping-exit</code> (управляемым опцией <code>-ping-exit</code>), <code>ping-restart</code> (управляемым опцией <code>-ping-restart</code>), <code>connection-reset</code> (запускается при перезагрузке TCP-соединения), <code>error</code> , or <code>unknown</code> (неизвестный сигнал). Эта переменная устанавливается непосредственно перед выполнением скрипта <code>down</code> .
time_ascii	Метка времени соединения клиента, отформатированная как строка, которую может прочитать человек. Устанавливается перед выполнением скрипта <code>-client-connect</code> .
time_duration	Продолжительность (в секундах) сеанса клиента, который сейчас отсоединяется. Устанавливается перед выполнением скрипта <code>-client-disconnect</code> .
time_unix	Метка времени соединения клиента, отформатированная как юниксовая целая величина даты/времени. Устанавливается перед выполнением скрипта <code>-client-connect</code> .

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

tls_id_n	Серия полей сертификатов от удаленного партнера, где n - уровень проверки. Устанавливается только для TLS-соединений. Устанавливается перед выполнением скрипта –tls-verify.
tls_serial_n	Серийный номер сертификата от удаленного партнера, где n - уровень проверки. Устанавливается только для TLS-соединений. Устанавливается перед выполнением скрипта –tls-verify.
tun_mtu	MTU устройства TUN/TAP. Устанавливается перед выполнением скрипта –up или –down.
trusted_ip	Действительный IP-адрес подключающегося клиента или партнера, который был аутентифицирован. Устанавливается перед выполнением скриптов –ipchange, –client-connect и –client-disconnect.
trusted_port	Действительный номер порта подключающегося клиента или партнера, который был аутентифицирован. Устанавливается перед выполнением скриптов –ipchange, –client-connect и –client-disconnect.
untrusted_ip	Действительный IP-адрес подключающегося клиента или партнера, который еще не был аутентифицирован. Иногда используется, чтобы выполнить функцию ptap для подключающегося хоста в скрипте –tls-verify, чтобы обеспечить правильную работу брандмауэра. Устанавливается перед выполнением скриптов –tls-verify и –auth-user-pass-verify.
username	Логин, предоставленный подключающимся клиентом. Устанавливается перед выполнением скрипта –auth-user-pass-verify, только когда указан модификатор via-env.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

X509_n_subject_field	<p>Поле X509 subject из сертификата удаленного партнера, где n - уровень проверки. Устанавливается только для TLS-соединений. Устанавливается перед выполнением скрипта – tls-verify. Эта переменная похожа на tls_id_n, за исключением того, что поля-компоненты X509 subject удалены, и никакого преобразования строк в значениях этих полей не происходит (за исключением преобразования управляющих символов в знак подчеркивания) Например, на сервере «OpenVPN-ГОСТ» при использовании образца клиентского сертификата из каталога sample-keys (client.crt) будут установлены следующие переменные (обратите внимание, что уровень проверки равен 0 для клиентского сертификата и 1 для сертификата УЦ):</p> <pre> X509_0_emailAddress=me@myhost.mydomain X509_0_CN=Test-Client X509_0_O=OpenVPN-TEST X509_0_ST=NA X509_0_C=KG X509_1_emailAddress=me@myhost.mydomain X509_1_O=OpenVPN-TEST X509_1_L=BISHKEK X509_1_ST=NA X509_1_C=KG </pre>
----------------------	--

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

8.13 Сигналы

SIGHUP	Заставляет «OpenVPN-ГОСТ» закрыть все сетевые соединения и соединения TUN/TAP, перезапуститься, перечитать конфигурационный файл (если есть) и заново открыть сетевые соединения и соединения TUN/TAP.
SIGUSR1	Похож на SIGHUP, за исключением того, что конфигурационный файл не перечитывается, и, возможно, не закрывается устройство TUN/TAP, перечитываются ключевые файлы, сохраняется локальный IP-адрес/порт, или сохраняется последний аутентифицированный удаленный IP-адрес/порт, основанные на опциях <code>-persist-tun</code> , <code>-persist-key</code> , <code>-persist-local-ip</code> , and <code>-persist-remote-ip</code> соответственно (см. выше). Этот сигнал также может быть сгенерирован внутри «OpenVPN-ГОСТ» состоянием таймаута под управлением опции <code>-ping-restart</code> . Этот сигнал в сочетании с опцией <code>-persist-remote-ip</code> может быть отправлен, когда подлежащие параметры сетевого интерфейса хоста меняются, например, когда хост - клиент DHCP и ему присвоен новый IP-адрес. Дополнительную информацию см. в описании опции <code>-ipchange</code> выше.
SIGUSR2	Заставляет «OpenVPN-ГОСТ» вывести свою текущую статистику (в файл <code>syslog</code> , если используется опция <code>-daemon</code> , в противном случае на стандартный вывод).
SIGINT, SIGTERM	Заставляет «OpenVPN-ГОСТ» корректно завершить работу.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения