КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-05 34 07 - ЛУ

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

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» в. 4.0

Средство защиты доступа к сетевым ресурсам «КриптоТуннель»

Руководство по использованию

СЕИУ.00009-05 34 07
Листов 48

Литера О

2022

Аннотация

Настоящий документ содержит руководство по использованию средства защиты доступа к сетевым ресурсам «КриптоТуннель» , которое представляет собой исполнение 5 (соответствует классу КС1) и исполнение 6 (соответствует классу КС2) СКЗИ «МагПро КриптоПакет» в. 4.0.

Содержание

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

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

1 Назначение программного комплекса

«МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» обеспечивает защищиту по крипторафическим алгоритмам ГОСТ соединения клиента с сервером при использовании практически любого прикладного протокола, работающего через TCP-соединение без динамического открытия портов, в частности HTTP, RDP, SMTP, POP3, IMAP, WebDAV, NFS, SQL и т.д.

Наиболее востребованным применением «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» является защита соединений с веб-серверами.

Отличительной особенностью «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» является возможность защитить соединения без существенного изменения настроек прикладного ПО.

«КриптоТуннель» — это составная часть СКЗИ «МагПро КриптоПакет» в. 4.0, а именно исполнение 5 (соответствует классу КС1) и исполнение 6 (соответствует классу КС2) указанного СКЗИ.

«КриптоТуннель» является функционально законченным изделием.

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

2 Условия работы программы

«КриптоТуннель» предназначена для работы в следующих операционных системах:

Windows 8.1/10;
Windows Server 2012/2016/2019;
Debian GNU/Linux 9(stretch)/10(buster)/11(bullseye);
Ubuntu 14.04, 16.04, 18.04, 20.04;
Linux Mint 19.x, 20.x, Linux Mint Debian Edition 4;
RedHat Enterprise Linux 7, 8;
CentOS 7, 8;
SUSE Linux 12, 15;
OpenSUSE 15.1, 15.2;
EMIAS OS 1.0, 2.0;
Дистрибутивы Альт на базе платформ 8 и 9, включая Альт Сервер, Альт Рабочая станция, Альт Рабочая станция К, Альт Образование, Альт 8 СП, Sipmly Linux;
МСВСфера Сервер 7.3, МСВСфера АРМ 7.3;
Гослинукс ІС6;
РЕД ОС 7.2, 7.3;
Rosa Enterprise Desktop (RED) X4;
Rosa Enterprise Linux Server (RELS) 7.3;
Rosa Enterprise Linux Desktop (RELD) 7.3;
РОСА КОБАЛЬТ;
Astra Linux Special Edition Смоленск 1.6 aka исп.1, 1.7;
Astra Linux Special Edition Новороссийск;
Astra Linux Common Edition 2.12;
Numa Edge 1.0;
FreeBSD 12.x, 13.x;
MacOS 10.15, 11;
Sun Solaris 10, 11;
OpenWRT 19.07, 21.02.

Для хранения закрыты ключей могу использоваться

- файловая система компьютера;
- любой аппаратный ключевой носитель, предоставляющий интерфейс PKCS#11 («Рутокен ЭЦП», «JaCarta» и им подобные);
- устройство «Рутокен» с хранением ключей в файловой системе токена;
- устройсво «Вьюга».

В будущем может быть добавлена поддержка и других устройств.

Из-за ошибки в системных библиотеках возможны проблемы при работе с ключами на аппаратных токенах в операционных системах SUSE Linux, ROSA RED и Альт.

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

3 Перечень функций

«МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» реализует защиту канала по протоколу TLS с использованием российских криптографических алгоритмов в соответствии с рекомендациями ТК26
Р 1323565.1.030-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)»;
Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;
МР 26.2.001-2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».

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

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» в. 4.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» в. 4.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» в. 4.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Правила пользования» (СЕИУ.00009–05 94).

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

5 Настройка

Для корректной работы всех компонентов «МагПро КриптоПакет» в. 4.0 необходимо, чтобы в общем конфигурационном файле openssl.cnf была корректно настроена загрузка энжина cryptocom, реализующего российские криптографические алгоритмы. Обычно этот файл содержит корректные настройки сразу после установки и в нём не требуется ничего менять. Если такая подтебнсоть всё-таки возникнет, руководствуйтесь разделом «Настройка» руководства по использованию утилиты openssl.

5.1 Настройка сервера

В данном разделе описывается минимальная настройка «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» на стороне сервера, полное описание всех параметров приведено в последующих разделах.

«КриптоТуннель» в серверной конфигурации выступает фронт-эндом перед защищаемым бэк-энд приложением: он принимает зашифрованное TLS-соединение от клиента и после выполнения собственных криптографических операций передаёт расшифрованные данные защищаемому приложению. Таким образом, на стороне сервера «КриптоТуннель» должен быть настроен на приём соединений из сети Интернет и передачу данных в безопасную внутреннюю сеть.

Для настройки «КриптоТуннель» на стороне сервера необходимо выполнить следующие действия:

1. Добавить в файл корфигурации *stunnel.conf* секции настройки удалённых подключений. Типовой вид секции настройки соединения с http-сервером:

```
[web-server]
protocol = http
client_auth = no
http_realip = no
http_forward = no
patch_hostname = yes
CAFile = .\crypto\ca.crt
cert = .\crypto\server.crt
key = .\crypto\server.key
sslVersion = TLSv1.2
ciphers = GOST2012-MAGMA-MAGMAOMAC
connect = 127.0.0.1:80
accept = 443
```

   Название секции выбирается произвольно. Рекомендуется устанавливать наиболее удобное для чтения журнала значение.
   Подпробное описание опций см. в разделе 5.6.

2. Если требуется аутентификация клиентов по сертификату, изменить значение параметра verifyChain на yes.

3. Выполнить формирование ключевой инфраструктуры в соответствии с описанием в разделе 5.8. Сформированные файлы расположить в соответствии с параметрами, указанными в *stunnel.conf*.

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

4. Для ОС Windows:
   - если «КриптоТуннель» установлен как служба, сделать рестарт службы stunnel;
   - выполнить перезапуск «КриптоТуннель» (исполняемый файл *starter.exe*).

   Для ОС семейства Linux/Unix: выполнить перезапуск stunnel.
5. Правильно настроить и запустить защищаемое приложение.

5.2 Настройка клиента

В данном разделе описывается минимальная настройка «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» на стороне клиента, полное описание всех параметров приведено в последующих разделах.

«КриптоТуннель» в клиентской конфигурации выступает в роли крипто-прокси, через который web-браузер или иное клиентское приложение соединяется с сервером. Он принимает соединение от клиента, зашифровывает его по протоколу TLS и «пробрасывает» к серверу. Таким образом, на стороне клиента «КриптоТуннель» должен быть настроен на приём локальных соединений и их передачу в сеть Интернет.

Для настройки «КриптоТуннель» на стороне клиента необходимо выполнить следующие действия:

1. Проверить параметры общей секции конфигурационного файла *stunnel.conf*. Необходимо, чтобы были установлены следующие значения:

   ```
   client = yes
   verifyChain = yes
   ```

2. Добавить секцию настройки удалённого подключения.
   Типовой вид:

   ```
   [someserver.ru]
   protocol = http
   accept = 8080
   connect = tls.someserver.ru:443
   sslVersion = TLSv1.2
   ciphers = GOST2012-MAGMA-MAGMAOMAC:GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
   CAFile = .\crypto\ca.crt
   TIMEOUTclose = 0
   ```

   Название секции выбирается произвольно. Рекомендуется устанавливать наиболее удобное для чтения журнала значение.
3. Если сервер требует аутентификации клиента по сертификату, в секции настройки удалённого подключения следует указать параметры вида:

   ```
   cert = [путь к файлу сертификатов пользователя в формате PEM]
   key = [путь к файлу закрытого ключа пользователя в формате PEM]
   ```

   Например, при стандартном наименовании и расположении файлов сертификата и закрытого ключа:

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

```
cert = .\crypto\client.crt
key = .\crypto\client.key
```

Описание ключевой инфраструктуры см. в разделе 5.8.

4. Для ОС Windows: При необходимости автоматического перехода на страницу сервера при запуске КриптоТуннель, добавить в секцию *urls* файла *starter.ini* параметры перехода на страницу:

```
; tls.someserver.ru
url_shop = http://127.0.0.1:8080/params.cgi
url_shop.title = Интернет-магазин
```

Подпробное описание процедуры см. в разделе 5.7.

5.3 Настройка работы через proxy

«МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» может работать через proxy, поддерживается работа как через прокси без автиризации пользователей, так и черех прокси с авторизацией пользователей по протоколам BASIC и NTML (однако протокол NTLMv2 не поддерживается).

Для настройки работы через прокси-сервер необходимо изменить строки секции следующим образом:

```
connect = <адрес прокси-сервера>:<порт>
protocol = connect
protocolProtocol = http
protocolHost = <адрес конечного TLS-сервера, с которым
                требуется установить соединение>
```

Если proxy-сервер требует авторизации пользователя по протоколу *basic*, то необходимо также указать дополнительные опции

```
protocolUsername = <имя пользователя на proxy-сервере>
protocolPassword = <пароль пользователя на proxy-сервере>
```

Если proxy-сервер требует авторизации пользователя по протоколу *ntlm*, то необходимо также указать дополнительные опции

```
protocolAuthentication = ntlm
protocolDomain = <имя домена Active Direcory>
protocolUsername = <имя пользователя на proxy-сервере>
protocolPassword = <пароль пользователя на proxy-сервере>
```

Подпробное описание опций см. в разделе 5.6.

5.3.1 Дополнительные настройка работы через proxy для ОС Windows

При использовании «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» на ОС Windows необходимо также добавить в секцию *updater* файла *starter.ini* параметр *proxy*. Если proxy-сервер работает без авторизации пользователей, следует использовать следующий формат задания параметра *proxy*:

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

```
proxy = <адрес прокси-сервера>:<порт>
```

Если proxy-сервер требует авторизации пользователей, следует использовать следующий формат задания параметра *proxy*:

```
proxy = <имя>:<пароль>@<адрес прокси-сервера>:<порт>
```

Если <имя> содержит знак двоеточия, его следует заменить на код %3A.

Подпробнее про файл *starter.ini* см. в разделе 5.7.

5.4 Настройка чтения ключа с устройства Рутокен

«МагПро КриптоПакет» в. 4.0 позволяет хранить закрытый ключ не только в файле, но и на устройсте Рутокен. Существует два способа хранения ключей на Рутокене: в файловой системе устройства или в неизвлекаемой памяти (второй вариант доступен только для устройств Рутокен ЭЦП и Рутокен PKI).

Ключ в файловой системе устройства должен быть создан средствами самого «МагПро КриптоПакет» в. 4.0.

Рутокен с ключом в неизвлекаемой памяти обычно приходит из Удостоверяющеего центра. Также можно создать такой ключ самостоятельно с помощью утилит из комплекта поставки Рутокена или средствами самого «МагПро КриптоПакет» в. 4.0.

Для использования ключа на устройстве Рутокен необходимо установить драйверы устройства (а при использовании ключей в неизвлекаемой памяти также библиотеку rtpkcs11ecp, предоставляющую интерфейс PKCS#11) и отредактировать файла конфигурации *stunnel.conf*, добавив в его общую секцию параметры

```
engine=auto
engineId=cryptocom
```

Для использования ключа в файловой системе Рутокена параметр **key** следует указывать следущим образом:

```
key=RUTOKEN:<id>
```

где <id> - идентификатор ключа на токене, использованный при его создании.

Для использования ключа в неизвлекаемой памяти Рутокена параметр **key** следует указывать следущим образом:

```
key=PKCS11:<label>
```

где <label> - метка ключа в неизвлекаемой памяти токена. Если в неизвлекаемой памяти токена записан только один ключ, метку можно не указывать.

5.5 Настройка чтения ключа с устройства JaCarta и других устройств, предоставляющих интерфейс PKCS#11

«МагПро КриптоПакет» в. 4.0 позволяет использовать закрытый ключ, расположенный в неизвлекаемой памяти устройства JaCarta, а также иных устройство, предоставляющих интерфейс PKCS#11. Совместно с «МагПро КриптоПакет» в. 4.0 допускается использовать только устройства, имеющие действующий сертификат ФСБ России.

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

Для использования таких ключей необходимо установить драйверы устройства, а также библиотеку, предоставляющую интерфейс PKCS#11 для этого устройства, и выставить переменную окружения `PKCS11_LIBNAME`, значением которой должен быть путь к этой библиотеке.

В общую секцию файла конфигурации *stunnel.conf* необходимо добавить параметры

```
engine=auto
engineId=cryptocom
```

Параметр **key** следует указывать следущим образом:

```
key=PKCS11:<label>
```

где <label> - метка ключа в неизвлекаемой памяти устройства. Если в неизвлекаемой памяти устройства записан только один ключ, метку можно не указывать.

5.6 Все опции конфигурационного файла *stunnel.conf*

Файл **stunnel.conf** является основным конфигурационным файлом программы. Он содержит в себе общую секцию и может включать несколько секций для настройки различных виртуальных хостов. Общая секция имеет обязательную часть в начале файла, которая, как правило, не требует изменений.

В конфигурационном файле допускаются:

- пустые строки (игнорируются).
- комментарии (игнорируются). Каждая строка комментария должна начинаться с символа ';' или '#'.
- строки вида «option_name = option_value».
- строки вида «[service_name]». Такая строка указывает на начало секции настройки сервиса.

Допускается использование опций защищённых соединений в общей секции. В таком случае эти опции будут применены ко всем дополнительным секциям.

5.6.1 Настройки общей секции

Общая секция может содержать следующие опции:

debug = LEVEL

уровень подробности сообщений лога

Отвечает за подробность лог-файла. Значение может быть именем или числом, соответствующим уровню сообщений.

Возможные значения: emerg (0), alert (1), crit (2), err (3), warning (4), alert (5), info (6) или debug (7). В логе будут отображаться все сообщения ниже или равные заданному уровню. Максимальный уровень *debug* = *debug* или *debug* = *7*. По умолчанию используется уровень 5.

При нормальной работе КриптоТуннеля не указывается.

engine = auto

необходима только при использовании ключей на аппаратных устройствах, этой опции следует указывать значение auto.

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

foreground = yes | quiet | no (только для Linux и Unix операционных систем)
режим работы

log = append | overwrite
режим работы с журналом

Позволяет выбрать режим работы с журналом: добавлять сообщения в журнал или при каждом запуске начинать журнал заново.

output = FILE
лог-файл приложения.

Указывает путь к лог-файлу приложения, в котором будет отображаться информация о подключениях и возможных ошибках.

pid = FILE (только для Linux и Unix операционных систем)
указывает на pid-файл.

service = SERVICE (только для Linux и Unix операционных систем)
имя службы КриптоТуннеля.

Указанное имя службы используется в системном журнале и в режиме inetd.

По умолчанию: stunnel

syslog = yes | no (только для Linux и Unix операционных систем)
задаёт ведение журнала через syslog.

По умолчанию: включено

5.6.2 Настройка параметров защищенных соединений

Настройка параметров защищенных соединений осуществляется в дополнительных секциях (отдельная секция для каждого соединения). Каждая секция должна начинаться с имени сервиса в квадратных скобках. Указанное имя позволит различать информацию сервисов в журнале программы. К именам сервисов не предъявляется никаких специальных требований, рекомендуется выбирать исходя из назначения соединения.

Настройка параметров защищенных соединений осуществляется заданием следующих опций конфигурационного файла stunnel.conf:

accept = [HOST:]PORT
принимать соединения по указанному адресу

Указывает адрес и порт, на которых КриптоТуннель будет ожидать подключения.
Допускается указывать только порт. В этом случае КриптоТуннель будет принимать соединения IPv4, пришедшие на указанный порт через любой сетевой интерфейс.
Для прослушивания всех адресов IPv6 следует использовать следующий формат:
accept = :::PORT

CApath = DIRECTORY
каталог сертификатов

Указывает папку, в которой КриптоТуннель будет искать сертификаты при использовании опций *verifyChain* и *verifyPeer*. Обратите внимание, что именование сертификатов в этой директории должно иметь вид XXXXXXXX.0, где XXXXXXXX - хеш поля subject в файле сертификата.

CAFile = CA_FILE

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

файл сертификата удостоверяющего центра

Указывает расположение файла сертификата (или набора сертификатов) удостоверяющего центра, которому КриптоТуннель будет доверять.

CRLpath = DIRECTORY

каталог списков отзыва сертификатов

Указывает папку, в которой КриптоТуннель будет искать CRL при использовании опций *verifyChain* и *verifyPeer*. Обратите внимание, что именование CRL в этой директории должно иметь вид XXXXXXXX.r0, где XXXXXXXX - хеш CRL.

CRLfile = CRL_FILE

файл списка отзыва сертификатов

Указывает расположение файла со списком отзыва (или набором списков отзыва) сертификатов.

cert = CERT_FILE

файл сертификата

Указывает расположение файла сертификата (или набора сертификатов) открытого ключа, используемого при установлении защищенного соединения. Файл может содержать всю цепочку сертификатов, начиная с фактического сертификата сервера/клиента и заканчивая самоподписанным сертификатом корневого УЦ. Файл должен быть в формате PEM или P12.

checkEmail = EMAIL

адрес электронной почты принимаемого сертификата

Если не заданы verifyChain или verifyPeer, то данная опция игнорируется. Допускается использование нескольких определений checkEmail в одной секции.
Сертификат будет принят, если адрес электронной почты, указанный в сертификате, совпадает с любым из адресов электронной почты, указанных в *checkEmail*.

checkHost = HOST

хост принимаемого сертификата

Если не заданы verifyChain или verifyPeer, то данная опция игнорируется. Допускается использование нескольких определений checkHost в одной секции.
Сертификат будет принят, если имя хоста, указанное в сертификате, совпадает с любым из хостов, указанных в *checkHost*.

checkIP = IP

IP-адрес принимаемого сертификата

Если не заданы verifyChain или verifyPeer, то данная опция игнорируется. Допускается использование нескольких определений checkIP в одной секции.
Сертификат будет принят, если IP-адрес, указанный в сертификате однорангового узла, совпадает с любым из IP-адресов, указанных в *checkIP*.

ciphers = CIPHER_LIST

задаёт список допустимых криптонаборов для TLS до версии 1.2 включительно.

Криптонаборы указываются через двоеточие. Допустимо использование следующих криптонаборов:
`GOST2012-MAGMA-MAGMAOMAC`,
`GOST2012-KUZNYECHIK-KUZNYECHIKOMAC`,
`GOST2012-GOST8912-GOST8912`,

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

`GOST2012-GOST8912-IANA`,
`GOST2001-GOST89-GOST89`
(последние три — только для обеспечения совместимости со старыми СКЗИ).

ciphersuites = CIPHER_LIST
задаёт список допустимых криптонаборов для TLS версии 1.3.

Криптонаборы указываются через двоеточие. Допустимо использование следующих криптонаборов:
`TLS_GOSTR341112_256_WITH_MAGMA_MGM_S`,
`TLS_GOSTR341112_256_WITH_MAGMA_MGM_L`,
`TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S`,
`TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L`.

client = yes | no
режим работы сервиса

По умолчанию no (работа в режиме сервера).

config = COMMAND [: PARAMETER]
команда настройки **OpenSSL**

Позволяет выполнять команды настройки **OpenSSL**.

connect = [HOST:] PORT
подключиться к указанному адресу

Указывает, куда КриптоТуннель направит соединение, пришедшее на адрес, указанный в accept. Если указан только порт, в качестве хоста будет использован localhost. При подключении к веб-серверу рекомендуется указывать то имя хота, которое веб-сервер счиитает своим именем.

curves = list
задаёт ECDH/GOST группы.

Группы указываются через двоеточие. Чтобы получить список поддерживаемых групп, выполните команду:

```
openssl ecparam -list_curves
```

По умолчанию используются следующие значения:
X25519:P-256:X448:P-521:P-384 (для OpenSSL 1.1.1 и более поздних версий)
prime256v1 (для OpenSSL старше версии 1.1.1)

debug = LEVEL
уровень подробности сообщений лога

Отвечает за подробность лог-файла. Значение может быть именем или числом, соответствующим уровню сообщений.
Возможные значения: emerg (0), alert (1), crit (2), err (3), warning (4), alert (5), info (6) или debug (7). В логе будут отображаться все сообщения ниже или равные заданному уровню. Максимальный уровень *debug* = *debug* или *debug* = *7*.

По умолчанию используется уровень 5.

delay = yes | no
отложить поиск DNS для опции **connect**

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

Этот параметр полезен для динамического DNS или когда DNS недоступен во время запуска КриптоТуннеля.
Данный режим автоматически включается, когда при запуске КриптоТуннель не может разрешить какой-либо из адресов подключения.

По умолчанию: выключено

engineId = cryptocom
задаёт энжин, который будет использован для доступа к ключу на аппаратном устройстве.

Для данной опции допустимо только значение **cryptocom**.

engineNum = ENGINE_NUMBER
задаёт номер энжина, который будет использован для доступа к ключу на аппаратном устройстве.

Нумерация энжинов начинается с 1.

exec = EXECUTABLE_PATH
выполнить локальную inetd программу.

На платформах Unix устанавливаются следующие переменные окружения:
`REMOTE_HOST`,
`REMOTE_PORT`,
`SSL_CLIENT_DN`,
`SSL_CLIENT_I_DN`.

execArgs = $0 $1 $2 ...
аргументы для **exec**, включая имя программы ($0).

Кавычки в настоящее время не поддерживаются. Аргументы разделяются произвольным количеством пробелов.

failover = rr | prio
задаёт стратегию обработки отказа для нескольких целей "connect".

rr круговая система - справедливое распределение нагрузки.

prio
использовать порядок указанный в конфигурационном файле.

По умолчанию: prio

ident = USERNAME
использовать проверку имени пользователя IDENT (RFC 1413).

include = DIRECTORY
использовать все части файла конфигурации, расположенные в DIRECTORY

Файлы подключаются в алфавитном порядке. Рекомендуемое соглашение об именах файлов:
для глобальных опций:
00-global.conf
для сервисов:
01-service.conf
02-service.conf

key = KEY_FILE
закрытый ключ сертификата, указанного в опции cert

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

Указывает расположение файла закрытого ключа, используемого при установлении защищенного соединения. Закрытый ключ необходим для аутентификации владельца сертификата. Поскольку этот файл должен храниться в секрете, он должен быть доступен для чтения только его владельцу. Этот параметр также используется в качестве идентификатора закрытого ключав случае использования аппаратных решений аутентификации (например, для ключей, хранящихся на RuToken).

libwrap = yes | no

задаёт использование /etc/hosts.allow и /etc/hosts.deny.

По умолчанию: отключено.

local = HOST

По умолчанию в качестве источника для удаленных подключений используется IP-адрес исходящего интерфейса. Используйте этот параметр для привязки статического локального IP-адреса.

logId = TYPE

задаёт тип идентификатора соединения.

Идентификатор служит для определения записей каждого из подключений в журнале. На данный момент поддерживаются следующие типы:

sequential

Числовой последовательный идентификатор, уникален только в пределах одного экземпляра КриптоТуннеля. Очень компактен, что наиболее полезно при ручном анализе журнала.

unique

Буквенно-цифровой идентификатор. Глобально уникален, но длиннее, чем порядковые номера *sequential*. Наиболее полезен при автоматическом анализе журнала.

thread

Идентификатор потока операционной системы. Не является ни уникальным (даже в пределах одного экземпляра КриптоТуннеля), ни коротким. Наиболее полезен во время отладки программного обеспечения или в случае проблем с конфигурацией приложения.

process

Идентификатор процесса операционной системы (PID). Может быть полезен в режиме inetd.

По умолчанию: sequential.

OCSP = URL

задаёт ответчик OCSP для проверки сертификата.

OCSPaia = yes | no

проверять сертификаты с их AIA OCSP ответчиками.

Этот параметр позволяет КриптоТуннелю проверять сертификаты со списком URL-адресов ответчика OCSP, полученным из их расширения AIA (доступ к информации о полномочиях).

OCSPflag = OCSP_FLAG

указывает флаг ответчика OCSP.

Для указания нескольких флагов опцию *OCSPflag* можно использовать повторно.

В настоящее время поддерживаются флаги:

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

```
NOCERTS,
NOINTERN,
NOSIGS,
NOCHAIN,
NOVERIFY,
NOEXPLICIT,
NOCASIGN,
NODELEGATED,
NOCHECKS,
TRUSTOTHER,
RESPID_KEY,
NOTIME.
```

OCSPnonce = yes | no

отправить и проверить расширение одноразового номера OCSP.

Этот параметр защищает протокол OCSP от повторных атак. В силу больших вычислительных затрат расширение nonce обычно обеспечивается только внутренними (например, корпоративными), а не общедоступными ответчиками OCSP.

options = SSL_OPTIONS

задаёт параметры библиотеки *OpenSSL*.

Параметр представляет собой имя опции *OpenSSL* в соответствии с руководством *SSL_CTX_set_options(3ssl)*, но без префикса *SSL_OP_*.
Команда *stunnel -options* перечисляет параметры, разрешенные в текущей версии КриптоТуннеля.
Для указания нескольких параметров опция может использоваться повторно. Перед именем параметра можно поставить тире ('-'), чтобы отключить параметр. Например, для совместимости с Eudora TLS можно использовать следующий вариант:

```
options = DONT_INSERT_EMPTY_FRAGMENTS
```

По умолчанию заданы опции:

options = NO_SSLv2
options = NO_SSLv3

Вместо отключения определенных версий протокола TLS при компиляции с OpenSSL 1.1.0 (или более поздней версии) используйте *sslVersionMax* или *sslVersionMin*.

protocol = PROTO

протокол приложения

В настоящее время поддерживаются протоколы:

cifs

Собственное (недокументированное) расширение протокола CIFS, реализованное в Samba. Поддержка этого расширения была прекращена в Samba 3.0.0.

connect

Соответствует RFC 2817 section 5.2 *(метод CONNECT для установления туннельного прокси-соединения)*.
Этот протокол поддерживается только в режиме клиента.

http

Указывает КриптоТуннелю, что защищаемый протокол - HTTP. В этом случае будут

доступны специфичные для этого протокола действия, например, передача клиентского сертификата на веб-сервер.

imap
Соответствует RFC 2595 *(Использование TLS с IMAP, POP3 и ACAP)*.

ldap
Соответствует RFC 2830 *(облегченный протокол доступа к каталогам (v3): расширение безопасности транспортного уровня)*.

nntp
Соответствует RFC 4642 *(Использование TLS с протоколом NNTP)*.
Этот протокол поддерживается только в режиме клиента.

pgsql
Соответствует
`http://www.postgresql.org/docs/8.3/static/protocol-flow.html`

pop3
Соответствует RFC 2449 *(Механизм расширения POP3)*.

proxy
Соответствует
`http://haproxy.1wt.eu/download/1.5/doc/proxy-protocol.txt`

rdp
Указывает, что защищаемый протокол - RDP.

smtp
Соответствует RFC 2487 *(расширение службы SMTP для безопасного SMTP через TLS)*.

socks
Поддерживаются версии 4, 4a и 5.
`http://www.openssh.com/txt/socks4.protocol`
`http://www.openssh.com/txt/socks4a.protocol`
Команда BIND протокола SOCKS не поддерживается. Параметр USERID игнорируется.

protocolAuthentication = AUTHENTICATION
тип аутентификации

Задаёт тип аутентификации для данного протокола. Используется только на стороне клиента протоколами *connect* и *smtp*.
Для протокола *connect* поддерживаются значения *basic* (используется по умолчанию) и *ntlm*.
Для протокола *smtp* поддерживаются значения *plain* (используется по умолчанию) и *login*.

protocolDomain = DOMAIN
имя домена

Задаёт имя домена Active Directory, используемого при работе через proxy с авторизацией по протоколу *ntlm*.
Используется только на стороне клиента и только с протоколом *connect*.

protocolHeader = HEADER

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

заголовок

Задаёт заголовок, используемый протоколом.

В настоящее время поддерживается только на стороне клиента и только с протоколом *connect*.

protocolHost = HOST:PORT

адрес подключения

Указывает конечный TLS-сервер, с котором требуется соединиться через прокси-сервер. Адрес прокси-сервера при этом задаётся опцией *connect*.

Используется только на стороне клиента протоколом *connect*.

protocolPassword = PASSWORD

пароль пользователя

Задаёт пароль пользователя при установлении соединения по указанному протоколу.

Используется только на стороне клиента протоколами *connect* и *smtp*.

protocolProtocol = *http*

Используется только на стороне клиента протоколом *connect* при туннелировании через прокси. Указывает КриптоТуннелю, что защищаемый протокол - HTTP. В этом случае будут доступны специфичные для этого протокола действия, например, передача клиентского сертификата на веб-сервер. Допускается использование только значения *http*. Любые другие значения игнорируются.

protocolUsername = USERNAME

имя пользователя

Задаёт имя пользователя при установлении соединения по указанному протоколу.

Используется только на стороне клиента протоколами *connect* и *smtp*.

PSKidentity = IDENTITY

Идентификатор PSK для PSK-клиента.

Опцию можно использовать на стороне клиента для выбора удостоверения PSK во время аутентификации. Эта опция игнорируется на стороне сервера.

По умолчанию: первое удостоверение, указанное в файле *PSKsecrets*.

PSKsecrets = FILE

файл с идентификаторами PSK и соответствующими ключами.

Каждая строка файла должна иметь вид:

```
IDENTITY:KEY
```

Шестнадцатеричные ключи автоматически преобразуются в двоичную форму. Ключи должны иметь длину не менее 16 байт (не менее 32 символов для шестнадцатеричных ключей). Должно быть установлено ограничение доступа к содержимому файла (на чтение и запись) для пользователей.

pty = yes | no (только для Linux и Unix операционных систем)

создаёт псевдотерминал для опции *'exec'*.

redirect = [HOST:]PORT

в случае непрохождения аутентификации по сертификату перенаправлять клиентские TLS-соединения на указанный адрес

Эта опция работает только в режиме сервера. Некоторые протоколы несовместимы с этой опцией.

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

renegotiation = yes | no
поддержка повторного согласования TLS.

Приложения повторного согласования TLS включают в себя некоторые сценарии аутентификации или изменения ключей для длительных соединений.
Следует учитывать, что эта функция может облегчить тривиальную DoS-атаку с перегрузкой ЦП:
`http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html`
Обратите внимание, что отключение повторного согласования TLS не полностью устраняет эту проблему.

По умолчанию: включено

reset = yes | no
для указания ошибок использовать флаг TCP RST.

На некоторых платформах эта опция не поддерживается.

По умолчанию: включено

retry = yes | no
повторно выполнить *connect+exec* в случае отключения.

По умолчанию: отключено

requireCert = yes | no
требовать сертификат клиента при установлении соединений

Используется только на стороне сервера. При установленном значении *no* (используется по умолчанию) сервер КриптоТуннеля будет устанавливать соединения с клиентами без сертификатов.
Опции *verifyChain = yes* и *verifyPeer = yes* подразумевают задание *requireCert = yes*.

securityLevel = LEVEL
задаёт уровень безопасности.

Значение каждого уровня описано ниже:
Уровень 0
Все разрешено.

Уровень 1
Уровень безопасности соответствующий минимум 80 битам безопасности. Любые параметры, обеспечивающие безопасность ниже 80 бит, исключаются. Таком образом ключи RSA, DSA и DH короче 1024 бит и ключи ECC короче 160 бит запрещены. Все экспортные криптонаборы запрещены, поскольку они предлагают менее 80 бит безопасности. SSL версии 2 запрещен. Любые криптонаборы, использующие MD5 для MAC, также запрещены.

Уровень 2
Уровень безопасности соответствующий 112 битам. Ключи RSA, DSA и DH короче 2048 бит, и ключи ECC короче 224 бит запрещены. В дополнение к исключениям уровня 1 любые криптонаборы, использующие RC4, также запрещены. SSL версии 3 не допускается. Сжатие отключено.

Уровень 3
Уровень безопасности соответствующий 128 битам. Ключи RSA, DSA и DH короче 3072 бит, и ключи ECC короче 256 бит запрещены. В дополнение к исключениям уровня 2 запрещены криптонаборы, не обеспечивающие прямой секретности. Версии

TLS ниже 1.1 запрещены. Мандаты сессий (session tickets) отключены.

Уровень 4
Уровень безопасности соответствующий 192 битам. Ключи RSA, DSA и DH короче 7680 бит и ключи ECC короче 384 бит запрещены. Криптонаборы, использующие SHA1 для MAC, запрещены. Версии TLS ниже 1.2 запрещены.

Уровень 5
Уровень безопасности соответствующий 256 битам. Ключи RSA, DSA и DH короче 15360 бит и ключи ECC короче 512 бит запрещены.

По умолчанию: 2.

Параметр *securityLevel* доступен только при компиляции с Криптопакетом версии 4.0 и более поздними версиями.

setgid = GROUP (только для Linux и Unix операционных систем)
Идентификатор группы.

В качестве глобальной опции: выполняет setgid() для указанной группы в режиме демона и убирает все остальные группы.

В качестве опции сервиса: устанавливает группу сокета Unix, указанного через *'accept'*.

setuid = USER (только для Linux и Unix операционных систем)
Идентификатор пользователя.

В качестве глобальной опции: выполняет setuid() для указанного пользователя в режиме демона.

В качестве опции сервиса: устанавливает владельца сокета Unix, указанного через *'accept'*.

sessionCacheSize = NUM_ENTRIES
Размер кэша сеанса.

sessionCacheSize задаёт максимальное количество записей внутреннего кэша сеанса.

Значение 0 соответствует неограниченному размеру. Не рекомендуется для использования из-за риска DoS-атаки с переполнением памяти.

sessionCacheTimeout = TIMEOUT
Время хранения кэша.

Задаёт количество секунд для хранения кэшированных TLS-сессий.

sessionResume = yes | no
Разрешает или запрещает возобновление сеанса.

По умолчанию: разрешено.

sessiond = HOST:PORT
Адрес sessiond TLS-сервера кэширования.

sni = SERVICE_NAME
В таком форате используется только а стороне клиента, задаёт значение, которое будет передано в расширении SNI протокола TLS. При отсутствии этой опции в расширении SNI будет передано значение из параметра connect. Для того, чтобы отключить передачу расширения SNI, задайте пустое значение в качестве SERVICE_NAME.

sni = SERVICE_NAME:SERVER_NAME_PATTERN
В таком формате используется только на стороне сервера.

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

Использование данного параметра позволяет серверу предоставлять несколько сертификатов на одном IP-адресе и TCP-порту, и, следовательно, позволяет работать нескольким сайтам (или другим сервисам поверх TLS) на одном IP-адресе без использования одного и того же сертификата на всех сайтах. Выбор сертификата осуществляется в зависимости от доменного имени, полученного в расширении SNI протокола TLS (см. описание параметра sni на стороне клиента).
Для того, чтобы настроить серверный КриптоТуннель для работы с несколькими сертификатами, нужно для каждого сертификата создать свою секцию. Одна секция будет главной, в ней задаются обычны папаметры соединения, в том числе может задаваться умолчательный сертфиикат. Секции для других сертификатов являются вспомогательными, в них указывается параметр sni, в котором SERVICE_NAME указывает на главную секцию, а SERVER_NAME_PATTERN задаёт доменное имя, при появлени которого в расширении SNI протокола TLS будут использоваться ключ и сертификат из этой вспомогательной секции. Это имя может начинаться с символа '*', например '*.example.ru', а также допускается указывать в одной вспомогательной секции несколько параметров sni.
Ниже приведён пример конфигурации с использованием SNI:

```
[virtual]
; основной сервис, принимающий соединения на указанном порту
accept = 443
connect = 80
cert =  default.pem
key  =  default-key.pem

[sni1]
; вспомогательный сервис 1
sni = virtual:server1.mydomain.ru
cert = server1.pem
key  = server1-key.pem

[sni2]
; вспомогательный сервис 2
sni = virtual:server2.mydomain.ru
cert = server2.pem
key  = server2-key.pem
verifyPeer = yes
CAfile = server2-allowed-clients.pem
```

socket = a|l|r:OPTION=VALUE[:VALUE]

настройка принимающего, локального или удалённого сокета

Примеры использования:

```
socket = l:SO_LINGER=1:60
    # установить тайм-аут на одну минуту для закрытия
      локального сокета
socket = r:SO_OOBINLINE=yes
    # размещать внеполосные (out-of-band) данные непосредственно
      в поток принимаемых данных для удаленных сокетов
```

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

```
socket = a:SO_REUSEADDR=no
    # отключить повторное использование адреса (по умолчанию
      включено)
socket = a:SO_BINDTODEVICE=lo
    # принимать соединения только по шлейфу (loopback interface)
```

sslVersionMin = SSL_VERSION

требует использовать протокол TLS не ниже указанной версии

Поддерживаются версии TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

sslVersionMax = SSL_VERSION

требует использовать протокол TLS не выше указанной версии

Поддерживаются версии TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

sslVersion = SSL_VERSION

требует использовать протокол TLS в точности указанной версии

Поддерживаются версии TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

stack = BYTES (кроме FORK конфигураций)

Размер стека создаваемых потоков.

Чрезмерный размер стека увеличивает использование виртуальной памяти. Недостаточный размер стека может привести к сбою приложения.

По умолчанию: 65536 байт (достаточно для всех протестированных платформ)

ticketKeySecret = SECRET

Шестнадцатеричный симметричный ключ, используемый для защиты конфиденциальности мандата сессии (session ticket).

Мандаты сессий, определенные в RFC 5077, обеспечивают расширенные возможности возобновления сессий, когда для поддержания сеанса на стороне сервера кэширование не требуется.

Комбинация параметров *ticketKeySecret* и *ticketMacSecret* позволяет возобновить согласованный сеанс на других узлах кластера или возобновить согласованный сеанс после перезапуска сервера.

Ключ должен иметь длину 16 или 32 байта (соответствует 32 или 64 шестнадцатеричным цифрам). Двоеточия могут дополнительно использоваться между двухсимвольными шестнадцатеричными байтами.

Эта опция работает только в режиме сервера.

Для поддержки мандатов в OpenSSL старше 1.1.1 требуется отключение параметра NO_TICKET. При этом следует учитывать, что этот параметр несовместим с параметром *redirect*.

ticketMacSecret = SECRET

Шестнадцатеричный симметричный ключ, используемый для защиты целостности мандата сессии (session ticket).

Ключ должен иметь длину 16 или 32 байта (соответствует 32 или 64 шестнадцатеричным цифрам). Двоеточия могут дополнительно использоваться между двухсимвольными шестнадцатеричными байтами.

Эта опция работает только в режиме сервера.

TIMEOUTclose = SECONDS

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

время ожидания close_notify

Рекомендуется устанавливать это значение в 0.

TIMEOUTconnect = SECONDS
время ожидания соединения с удалённым хостом

TIMEOUTbusy = SECONDS
время ожидания запрошенных данных

TIMEOUTidle = SECONDS
время удержания бездействующего соединения

transparent = none | source | destination | both (только для Linux и Unix операционных систем)
Включает поддержку прозрачных прокси на выбранных платформах.

Поддерживаемые значения:

none
Отключает поддержку прозрачных прокси. Задано по умолчанию.

source
Подменяет адрес так, чтобы он выглядел так, как-будто подключение идёт с клиента TLS, а не с компьютера, на котором работает КриптоТуннель.

destination
В качестве адреса подключения используется исходный пункт назначения.

both
Использование как *source*, так и *destination* прозрачных прокси.

Для обратной совместимости поддерживается два устаревших варианта:

yes
соответствует значению *source*.

no соответствует значению *none*.

verifyChain = yes | no
аутентификация по цепочке сертификатов

Выполняет аутентификацию хоста с проверкой всей цепочки сертификатов до корневого УЦ.
При проверке сертификата сервера также важно использовать опции *checkHost* или *checkIP*.
Самоподписанный корневой сертификат УЦ должен храниться либо в файле, указанном в CAfile, либо в каталоге, указанном в CApath.
По умолчанию опция выключена.

verifyPeer = yes | no
аутентификация по заранее известному сертификату

Требует, чтобы полученный от второй стороны сертификат совпадал с сертификатом, который хранится либо в файле, указанном в CAfile, либо в каталоге, указанном в CApath.
По умолчанию опция выключена.

verify = LEVEL определяет,какие проверки сертификата второй стороны будут производится, может принимать 5 значений:

0 сертификат клиента проверяться не будет, использование этого значения на стороне сервера означает, что к КриптоТуннелю сможет подключиться любой пользователь

на совместимом ПО. Использовать это значение на стороне клиента категорически не рекомендуется;

1 сертификат будет проверяться, если другая сторона его предоставит. Промежуточный вариант между 0 и 2, использовать это значение на стороне клиента категорически не рекомендуется;

2 сертификат второй стороны будет требоваться и проверяться с использование сертификата УЦ и, при необходимости, промежуточных сертификатов (цепочки сертификатов), расположение которых указано в CAFile или CApath. Если сертификат истёк, выдан не доверенным УЦ, его нет и т.д., соединение будет отвергнуто сервером.
Эквивалентно verifyChain=yes

3 дополнительно к проверке сертификата, соответствующей verify=2, проверяется, что предъявленный второй стороной сертификат содержится в файле CAFile или каталоге CApath
Эквивалентно verifyChain=yes и verifyPeer=yes

4 проверяется, что предъявленный второй стороной сертификат содержится в файле CAFile или каталоге CApath, при этом проверка самого сертификата не производится.
Эквивалентно verifyPeer=yes

5.6.3 Настройка HTTP параметров защищённых соединений

Опции, доступные только при использовании протокола HTTP (*protocol* = *http*):

buffer_size = BUFFSIZE
задаёт размер буфера обмена в килобайтах
При нормальной работе КриптоТуннеля не указывается.

client_auth = yes | no
вставляет в HTTP-сообщение заголовок X509-Cert
Этот заголовок содержит сертификат пользователя, который авторизовался на сервере. Если HTTP-сообщение уже содержит заголовок X509-Cert, будет выполнена его замена на реальное значение.
Используется только на стороне сервера. По умолчанию опция отключена.

http_forward = yes | no
установливает значение заголовка X-Forwarded-For в HTTP-запросах
Добавляет в поле X-Forwarded-For заголовка HTTP-запроса IP-адрес хоста, с которым установлено соединение.
По умолчанию опция включена (значение yes).

http_merge_packages = yes | no
указывает КриптоТуннелю объединять пакеты заголовков HTTP-сообщений
При нормальной работе КриптоТуннеля не указывается.
По умолчанию опция включена (значение yes).

http_realip = force | yes | no
установливает значение заголовка X-Real-IP в HTTP-запросах
Значение будет соответствовать IP-адресу хоста, с которым установлено соединение.
Если *http_realip* = *yes*, но при этом в запросе уже присутствует заголовок X-Real-IP, то значение заголовка не будет изменено. Если *http_realip* = *force*, то значение заголовка

всегда определяется КриптоТуннелем.
По умолчанию опция выставлена в значение yes.

patch_hostname = yes | no
указывает КриптоТуннелю менять значение заголовка Host в HTTP-запросах
Значение заголовка Host в запросах клиента будет заменено на значение, соответствующее опции *connect*. В случае туннелирования через прокси будет использовано значение, соответствующее опции *protocolHost*. При нормальной работе КриптоТуннеля не указывается.
По умолчанию включена.

patch_location = yes | no
указывает КриптоТуннелю менять значение заголовка Location в ответах web-сервера
При нормальной работе КриптоТуннеля не указывается.
По умолчанию включена.
Учитывается только в клиентской конфигурации, в случае серверной конфигурации игнорируется, т.е. модификация заголовков Location производится, даже если опция выставлена в no.

5.7 Все опции конфигурационного файла *starter.ini*

Данный раздел актуален ТОЛЬКО для ОС семейства Windows. В других ОС данный файл не используется.

Конфигурационный файл **starter.ini** отвечает за настройку приложения *starter.exe*. Формат файла соответствует формату ini-файлов ОС Windows.

5.7.1 Секция общих настроек *common*

За общие настройки приложения отвечает секция *common*, которая может содержать следующие опции:

warning_days = DAYS
Указывает за сколько дней уведомлять пользователя об окончании срока действия лицензии. По умолчанию уведомление пользователя производится за 7 дней.

5.7.2 Секция *urls*

Редактировать секцию *urls* необходимо ТОЛЬКО на стороне клиента. Данная секция используется для указания http-страниц, на которые следует перейти после установления защищенного соединения с серверами, а также для указания удобных алиасов этих страниц и приложений, используемых для их просмотра. Если необходимости в переходе на определённые http-страницы сразу после запуска starter.exe нет, то заполнять данную секцию не требуется.

Настройка переходов на http-страницы осуществляется указанием следующих опций:

url_name = VALUE
задаёт url сервера (ссылка на http-страницу)

url_name.title = ALIAS
алиас сервера

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

url_name.open = APP_PATH
путь к приложению для просмотра содержимого страницы

Для настройки перехода на http-страницу требуется:

1. Выбрать уникальный идентификатор страницы *url_name*;
2. Добавить в конфигурационный файл строку *url_name* = *URL*, где URL имеет вид http://127.0.0.1:[номер локального порта]/<имя страницы на сервере>;
3. Добавить в конфигурационный файл строку *url_name.title* = <*алиас сервера*> (указывать не обязательно);
4. Добавить в конфигурационный файл строку *url_name.open* = <*путь к приложению для просмотра страницы*> (указывать не обязательно).

Идентификатор *url_name* выбирается произвольно. К идентификаторам *url_name* имеются 2 требования:

1. Идентификатор ДОЛЖЕН быть уникальным (для настройки разных страниц использовать разные идентификаторы; для настройки перехода на одну и ту же страницу использовать один и тот же идентификатор);
2. Идентификатор НЕ ДОЛЖЕН содержать пробелов и точек.

При работе пользователя с «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» в контекстом меню, которое пользователь вызывает щелчком правой кнопки мыши по иконке «КриптоТуннель» в трее, выводится именно список алиасов серверов. Этот же список выводится в качестве меню при запуске «КриптоТуннель» , если в нём более одного алиаса.

Имя страницы на сервере указывается в том случае, если после установления TLS-соединения с сервером пользователю необходимо попасть не на корневую страницу сервера, а на какую-либо другую. Указание имени страницы необязательно. Если его не указывать, пользователю будет предоставлена корневая страница сервера.

Путь к приложению для просмотра http-страницы указывать не обязательно. В этом случае для перехода на страницу будет запущено используемое по умолчанию приложение (браузер).

Пример секции urls для соединения с двумя серверами:

```
[urls]
; tls.someserver.ru
url_shop = http://127.0.0.1:8080/params.cgi
url_shop.title = Интернет-магазин

; tls.anotherserver.ru
url_bank = http://127.0.0.1:8083
url_bank.title = Интернет-банк
url_bank.open = C:\Program Files\Internet Explorer\iexplore.exe
```

Здесь знаком ';' помечены произвольные комментарии.

Строка с алиасом «Интернет-магазин» соответствует серверу tls.someserver.ru, т.к. для нее указан порт 8080 на 127.0.0.1, который в файле stunnel.conf указан как соответствующий серверу tls.somserver.ru; далее указана страница params.cgi. В результате при установлении tls-соединения с сервером tls.somserver.ru пользователь увидит страницу params.cgi на сервере tls.someserver.ru.

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

Строка с алиасом «Интернет-банк» соответствует серверу tls.anotherserver.ru, т.к. для нее указан порт 8083 на 127.0.0.1, который в файле stunnel.conf указан как соответствующий серверу tls.anotherserver.ru. Далее никаких страниц не указано, что означает, что при установлении tls-соединения пользователь увидит корневую страницу сервера tls.anotherserver.ru. Для данной страницы отдельно указано, что открывать её требуется приложением Internet Explorer. Таким образом просмотр данной страницы будет выполнен именно этим браузером, независимо от того, какое приложение используется в системе для просмотра http-страниц по умолчанию.

5.7.3 Секция *updater*

Данная секция используется для задания параметров получения и обновления лицензии. Секция может содержать следующие опции:

address = URL
: задаёт адрес сервера, к которому программа обратиться за лицензией при её получении по лицензионному ключу (см. раздел 6.1.2).

proxy = [user:password]@host:port
: Задает адрес и номер порта proxy-сервера, если доступ к серверу, указанному в параемтре **address**, должен осуществляться через proxy. Также может задавать имя и пароль для авторизации на proxy-сервере, если сервер требует авторизацию.

delay = VALUE
: указывает задержку отображения прогресс-индикации при получении или обновлении лицензии. Обычно процесс получения/обновления лицензии завершается очень быстро и не требует прогресс-индикации, поэтому прогресс-индикатор начинает отображаться не сразу, а через указанное в данном параметре время.
Если VALUE меньше 600, оно трактуется как секунды, если больше 600, то как миллисекунды.
Значение по умолчанию - 2 секунды.

5.8 Ключевая инфраструктура

5.8.1 Серверная ключевая инфраструктура

Для того, чтобы «КриптоТуннель» в серверной конфигурации мог устанавливать защищенные соединения с клиентами по протоколу TLS, на сервере необходимо установить TLS-сертификат, который будет использоваться для аутентификации сервера, и соответствующий ему закрытый ключ. Кроме того, необходим корневой сертификат удостоверяющего центра.

Сертификат сервера, соответствующий ему закрытый ключ и корневой сертификат УЦ следует установить на сервере в соответствии с конфигурационным файлом «КриптоТуннель» (файл *stunnel.conf* в каталоге установки). Кроме того, корневой сертификат УЦ должен быть предоставлен всем клиентам, которые будут устанавливать защищенные соединения с данным сервером.

TLS-сертификат сервера должен отвечать следующим требованиям:

1. Если на веб-сервере расположен один виртуальный сайт, то сертификат данного сервера должен содержать DNS-имя данного сайта в поле CN субъекта. Если же на веб-сервере

расположены несколько виртуальных сайтов, то сертификат такого сервера должен содержать расширение Subject Alternative Name. В этом расширении должны быть прописаны DNS-имена всех виртуальных сайтов, которые будут доступны по защищенному соединению, в формате:
DNS:<сайт 1>,DNS:<сайт 2>, ...DNS:<сайт N>
Возможно также использование на одном сервере нескольких сертификатов и соответствующих им закрытых ключей, подробнее об этом см. описание параметра **sni** в разделе 5.6.2.

2. Сертификат сервера должен содержать расширение Enhanced Key Usage со значением *Server Authentication (1.3.6.1.5.5.7.3.1)*.

5.8.2 Клиентская ключевая инфраструктура

Если при установлении защищенного соединения требуется также и клиентская аутентификация, необходимо создать TLS-сертификат и соответствующий ему закрытый ключ для каждого клиента. Сертификат клиента ДОЛЖЕН содержать расширение Enhanced Key Usage со значением *Client Authentication (1.3.6.1.5.5.7.3.2)*.

5.8.3 Формат файлов ключевой информации

Все файлы ключевой информации, как серверные, так и клиентские, должны быть в формате PEM.

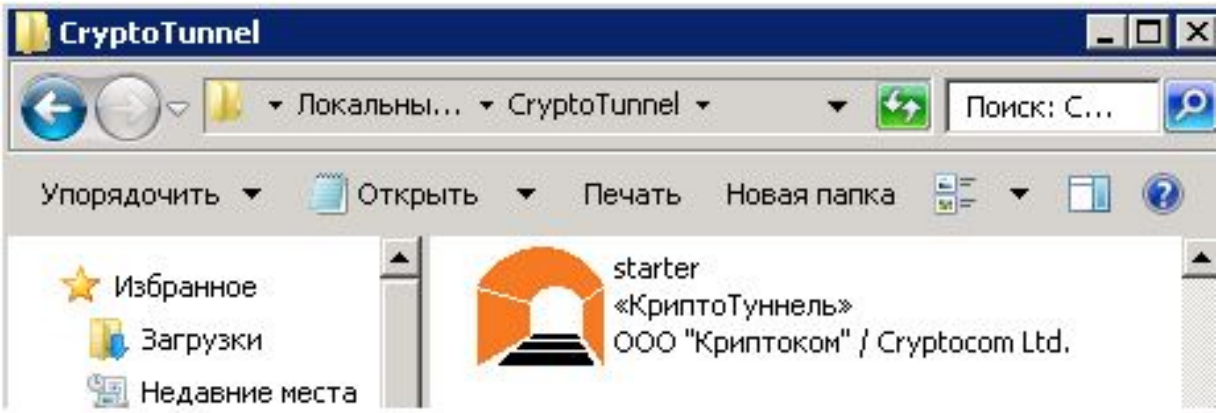
6 Использование

6.1 Использование в ОС семейства Windows

6.1.1 Запуск «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель»

Запуск «КриптоТуннель» осуществляется программой *starter.exe*. Как правило, в серверном исполнении ярлык на данный файл создаётся автоматически во время установки и помещается на рабочий стол, поэтому оператору для начала работы достаточно дважды щёлкнуть мышью по соответствующей иконке. В остальных случаях запуск осуществляется через окно «Мой компьютер». Для этого необходимо:

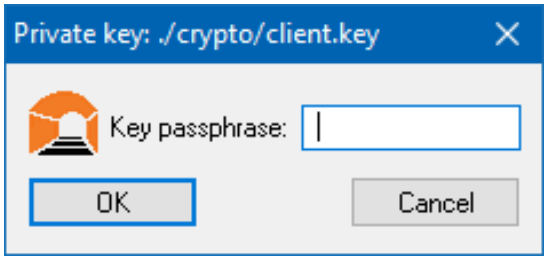
1. В случае установки программного комплекса «КриптоТуннель» на внешнем носителе (flash-устройство или лазерный диск) подключить этот носитель к компьютеру.
2. Через «Мой компьютер» перейти в папку с «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» :



3. Запустить «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» , дважды щелкнув мышью по иконке starter.

При первом запуске будет вызвана программа инициализации генератора случайных чисел gmkseed (подробности см. в документации на эту программу).

Если закрытый ключ сервера/пользователя, указанный в конфигурационном файле *stunnel.conf*, защищен PIN-кодом, то после запуска «КриптоТуннель» появится окно запроса PIN-кода ключа:



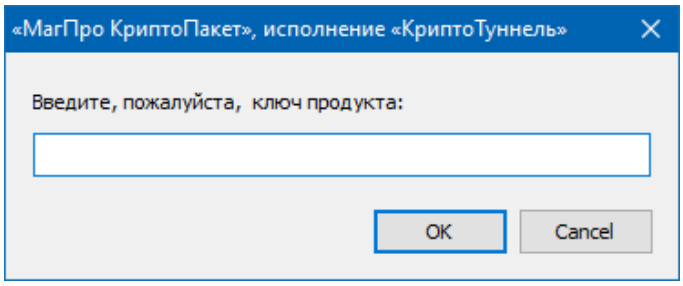
В заголовке окна присутствует строка, соответствующая расположению ключа, для которого запрашивается PIN-код. Оператору в поле ввода необходимо указать PIN-код ключа и нажать кнопку OK.

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

6.1.2 Лицензирование

6.1.2.1 Ввод лицензии

При первом запуске *starter.exe* появится окно ввода ключа продукта:



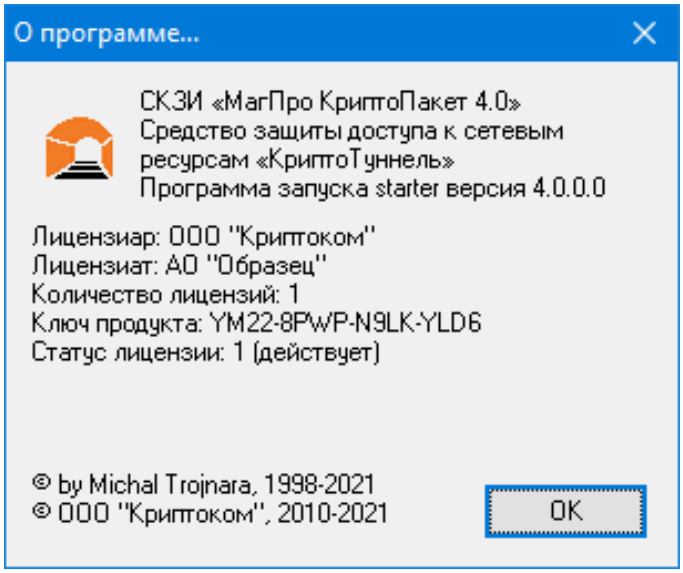
От оператора требуется ввести ключ продукта и нажать кнопку «ОК».

При наличии лицензии в системе этот запрос не отображается.

Предоставляемая лицензия может иметь ограниченный период действия и регулярно автоматически обновляется. Обычно обновление лицензии происходит за 8 дней до окончания её действия. Если этого по каким-то причинам не призойдет, за несколько (по умолчанию, 5) дней до окончания срока действия лицензии при запуске «КриптоТуннель» будет появляться соответствующее предупреждение. Количество дней определяется настройками программы (опция *warning_days* в файле *starter.ini*. При появлении такого сообщения необходимо выявить и устранить причины, мешающие автоматическому обновлению лицензии.

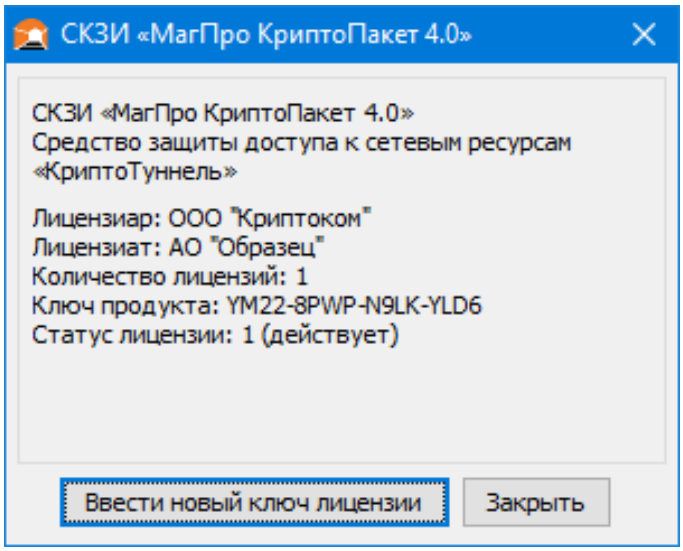
6.1.2.2 Просмотр сведений о лицензии

Для просмотра сведений о текущей лицензии необходимо выбрать пункт «О программе...» контекстного меню. В этом случае откроется окно, содержащее сведения о продукте и лицензии:



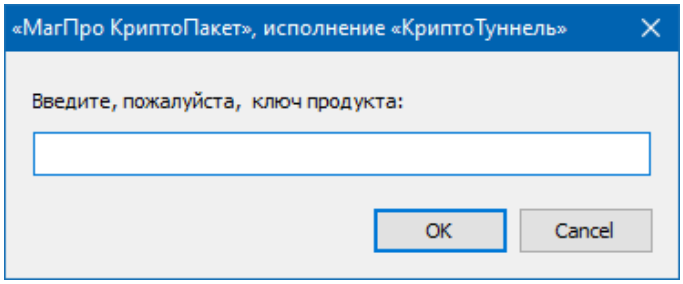
Альтернативный способ - открыть окно журнала (см.6.1.5), выбрать пункт меню «Помощь» и в выпадающем подменю - пункт «Лицензия». В это случае окно с информацией о лицензии будет иметь вид

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

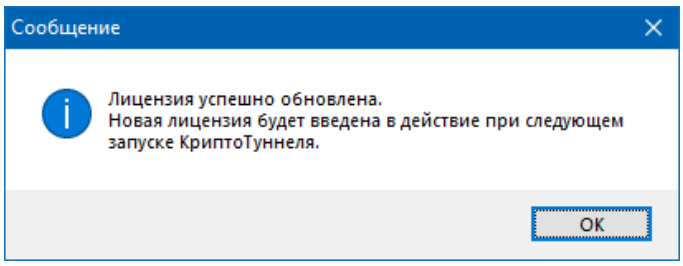


6.1.2.3 Смена лицензии

Если Вы использовали временную тестовую лицензию, а потом приобрели постоянную, Вам необходимо ввести в программу новый лицензионный ключ. Для этого в описанном выше окне просмотра информации о лицензии необходимо нажать на кнопку «Ввести новый лицензионный ключ». Появится окно ввода ключа продукта:



От оператора требуется ввести ключ продукта и нажать кнопку «OK». После получения новой лицензии появится сообщение

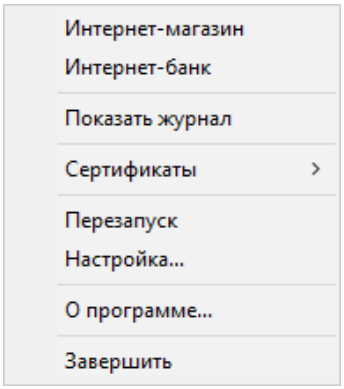


Для того, чтобы новая лицензия вступила в действие, необходимо завершить работу КриптоТуннеля и запустить его заново.

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

6.1.3 Контекстное меню

Контекстное меню «КриптоТуннель» появляется при щелчке правой клавишей мыши на иконке в трее:



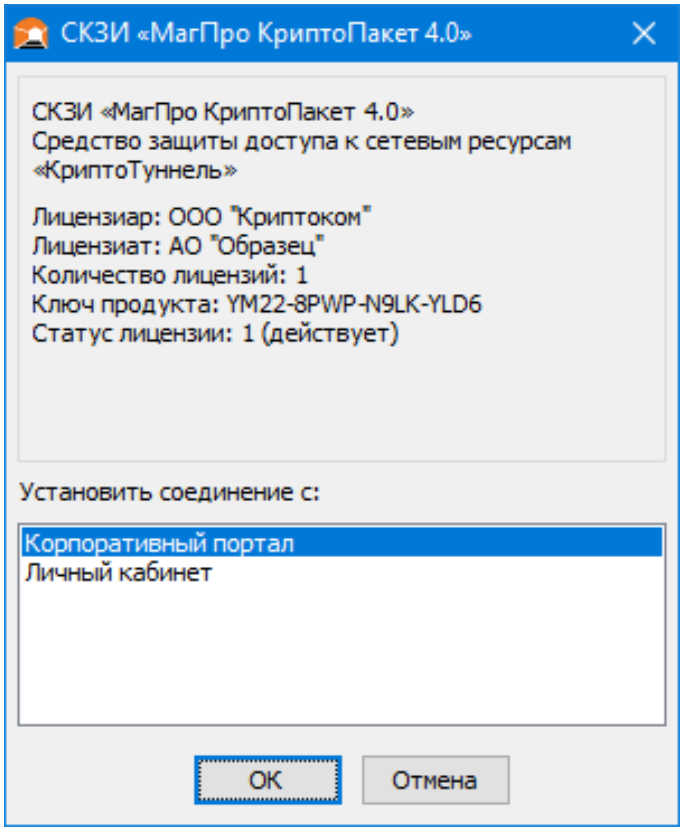
Контекстное меню состоит из двух частей. В верхней части выводится список алиасов http-страниц, на которые можно перейти после установления защищённого соединения (см. 5.7.2). В нижней части выводятся служебные пункты:

Показать журнал — открывает журнал программы
Сертификаты — позволяет сохранять сертификаты объектов, с которыми установлено защищённое соединение
Перезапуск — выполняет перезапуск «КриптоТуннель»
Настройка — открывает конфигурационный файл *stunnel.conf* в редакторе
О программе... — открывает окно, содержащее сведения о продукте
Завершить — завершает работу программы

6.1.4 Переход на http-страницы защищаемых объектов

Если в конфигурационном файле starter.ini в секции urls указана только одна страница перехода, то при запуске «КриптоТуннель» автоматически запустится браузер, в котором открывается необходимая пользователю страница.

Если в конфигурационном файле starter.ini в секции urls указано более одной страницы перехода, то выводится окно, в верхней части которого отображается информация о продукте и лицензии, а в нижней — меню, предоставляющее выбор объекта:



В данном примере указаны алиасы двух http-страниц — Интернет-магазин и Интернет-банк.

Следует щелкнуть мышью по названию необходимого объекта и нажать на кнопку «ОК». Запустится браузер, в котором откроется необходимая пользователю страница. Если нажать кнопку «Отмена», браузер не будет открыт, но «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» продолжит работу, иконка в трее остается.

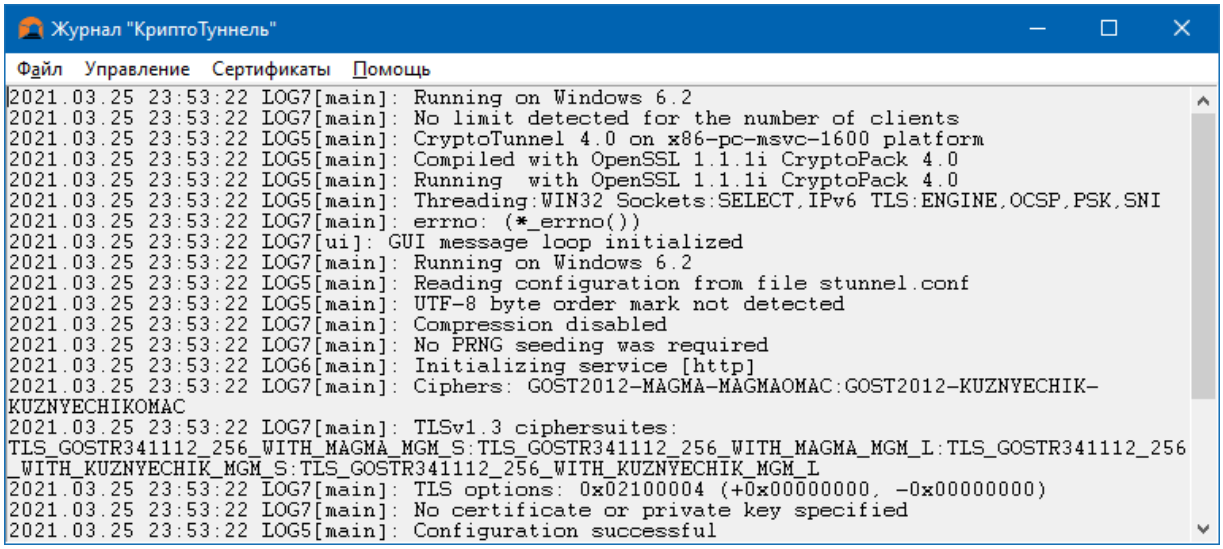
Помимо описанных выше способов, перейти на нужную страницу можно через контекстное меню, щёлкнув правой кнопкой мыши по иконке «МагПро КриптоПакет» в. 4.0 в трее. В контекстном меню в верхней его части будут содержаться пункты, названия которых соответствуют алиасам страниц, указанных в секции *urls* файла *starter.ini*. Для перехода на нужную страницу следует щелкнуть левой кнопкой мыши по соответствующему пункту.

6.1.5 Журнал работы «КриптоТуннель»

Журнал работы «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» содержит информацию о последних операциях (ограничено 1000 строками), выполненных «КриптоТуннель» с момента последнего запуска. Эта информация может быть полезна для системного администратора при возникновении каких-либо ошибок при работе «КриптоТуннель» .

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

Для того, чтобы просмотреть журнал работы «КриптоТуннель» , необходимо щелкнуть правой кнопкой мыши по иконке «КриптоТуннель» в трее. В появившемся контекстом меню выбрать пункт «Показать журнал». Выводится журнал работы «КриптоТуннель» :



Следует сохранить содержание журнала в текстовый файл, воспользовавшись пунктом «Сохранить лог как...» меню «Файл» в левом верхнем углу окна журнала, и предоставить файл системному администратору.

Полный лог сообщений «КриптоТуннель» пишется в файл, задаваемый опцией *output* конфигурационного файла *stunnel.conf* (см. раздел 5.6).

Следует помнить, что ошибки «КриптоТуннель» , связанные с неверной конфигурацией, также сохраняются в специальный лог-файл *stunnel.start.log* в папке программы.

Для того, чтобы просто убрать с экрана окно просмотра журнала, следует нажать на кнопку «Свернуть» (подчерк) в правом верхнем углу окна, в то время как нажатие на кнопку «Закрыть» (крестик) приведёт к завешению работы программы.

6.1.6 Выход из программы

Выход из программы можно осуществить через контекстное меню, меню окна просмотра журнала и кнопки управления окном просмотра журнала.

Для завершения работы программы через контекстное меню необходимо в меню найти пункт «Завершить» и щёлкнуть по нему левой кнопкой мыши.

Для завершения работы программы через меню окна просмотра журнала необходимо выбрать пункт меню «Файл» и в выпадающем подменю – пункт «Завершить».

Для завершения работы программы через кнопки управления окном просмотра журнала необходимо нажать на кнопку «Закрыть» (крестик) в правом верхнем углу окна и в появившемся запросе подтверждения нажать кнопку «Да».

При запуске «КриптоТуннель» со съёмного носителя в контекстном меню рядом с пунктом «Завершить» появится дополнительный пункт «Завершить и извлечь». Он служит для завершения программы и подготовки съёмного носителя к безопасному извлечению. После щелчка мышью по данному пункту съёмный носитель можно будет извлечь из системы.

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

6.1.7 Служба «КриптоТуннель»

Данный раздел содержит информацию по использованию продукта в случае установки «КриптоТуннель» в качестве системной службы.

После выполнения процедуры настройки служба «КриптоТуннель» готова к работе. Необходимо помнить, что для того, чтобы настройки вступили в силу, требуется выполнять перезапуск службы *stunnel*.

Если во время запуска службы возникают ошибки, связанные с неверной конфигурацией, то будет сформирован специальный лог-файл *stunnel.start.log*, включающий соответствующие сообщения. Сообщения о прочих ошибках, возникающих при работе службы, добавляются в основной журнал (задаётся опцией *output*).

При использовании службы «КриптоТуннель» на стороне клиента для установления соединения с web-сервером, защищённым по протоколу TLS с использованием алгоритмов ГОСТ, в адресной строке браузера небходимо в ввести *адрес:порт*, указанные в файле конфигурации опцией *accept*.

6.2 Использование в UNIX-подобных ОС

6.2.1 Подготовка к работе

В случае использования программного датчика случайных чисел перед первым запуском «МагПро КриптоПакет» в. 4.0 в исполнении «КриптоТуннель» необходимо создать файл инициализации программного ДСЧ. Для этого необходимо запустить программу

```
sudo -H /opt/cryptopack4/bin/mkseed
```

и следовать её указаниям (подробнее см. «Программа генерации файла инициализации программного ДСЧ mkseed. Руководство по использованию»).

После создания файла начального заполнения программного ДСЧ и выполнения процедуры настройки, описанной в разделе 5, «КриптоТуннель» готов к работе.

6.2.2 Запуск «КриптоТуннеля»

В ОС Linux запуск осуществляется командой

```
sudo -H systemctl start stunnel-gost
```

В ОС FreeBSD запуск осуществляется командой

```
sudo -H /etc/rc.d/stunnelgost start
```

В ОС Solaris запуск осуществляется командой

```
sudo -H /etc/init.d/stunnel-gost start
```

В macOS запуск осуществляется командой

```
sudo -H /opt/stunnel-gost/bin/start_stop start
```

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

6.2.3 Использование «КриптоТуннеля»

При использовании «КриптоТуннель» на стороне клиента для установления соединения с web-сервером, защищённым по протоколу TLS с использованием алгоритмов ГОСТ, в адресной строке браузера небходимо в ввести *адрес:порт*, указанные в файле конфигурации опцией *accept*.

6.2.4 Управление «КриптоТуннелем»

Для управления туннелем в среде Unix можно использовать следующие сигналы:

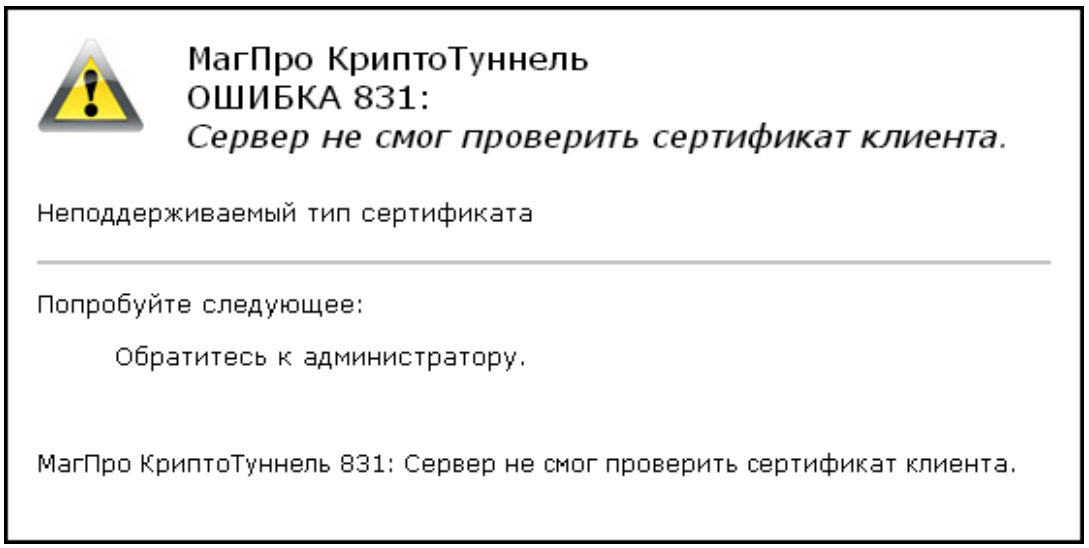
SIGHUP	Принудительно перезагрузить файл конфигурации. Следующие глобальные параметры не будут перезагружены: – chroot – foreground – pid – setgid – setuid Использование опции setuid также предотвратит подключение «КриптоТуннеля» к привилегированным (<1024) портам во время перезагрузки конфигурации. Если используется опция chroot, <КриптоТуннель» будет искать все свои файлы (включая файл конфигурации, сертификаты, файл журнала и файл pid) внутри «тюрьмы» chroot.
SIGUSR1	Закрыть и повторно открыть файла журнала «КриптТуннеля». Этот сигнал можно использовать при выполнении log rotation.
SIGUSR2	Вывести список активных подключений.
SIGTERM, SIGQUIT, SIGINT	Закрыть туннель

Результат отправки любых других сигналов на сервер не определен.

7 Сообщения оператору

7.1 Общие замечания

Если при работе «МагПро КриптоПакет» в. 4.0 возникает ошибка, в браузере на стороне клиента появится страница с сообщением об ошибке, например:



Крупными буквами выводятся код и характеристика ошибки, ниже — возможная причина и действия, которые следует предпринять для исправления ошибки.

Если в качестве действия, которое следует предпринимать для исправления ошибки, указано «обратитесь к администратору сервера», следует обращаться к администратору того сервера, с которым Вы пытаетесь установить соединение.

7.2 Ошибки при попытке установить соединение

Код ошибки	**Ошибка**	**Причина**	**Действия оператора**
717	Не удалось определить адрес сервера по его DNS имени	Возможно, отсутствует подключение к Интернету, или в конфигурационном файле имя сервера написано с ошибкой.	Проверьте, что компьютер подключен к Интернету. Если проблема сохранилась, проверьте, правильно ли отредактирован основной конфигурационный файл *stunnel.conf* (см. раздел 5) и при необходимости внесите исправления.
813	Нет доверия к сертификату сервера, потому что срок его действия еще не наступил	Возможно, действительно срок действия сертификата еще не наступил. Или же на Вашем компьютере установлена неправильная дата.	Проверьте, что на Вашем компьютере уставлена правильная дата. Если дата правильная, следует обратиться к администратору сервера и проинформировать его о проблемах с используемым на сервере сертификатом.
814	Нет доверия к сертификату сервера, потому что срок его действия истек	Возможно, действительно истек срок действия сертификата сервера. Или же на Вашем компьютере установлена неправильная дата.	Проверьте, что на Вашем компьютере уставлена правильная дата. Если дата правильная, следует обратиться к администратору сервера и проинформировать его о проблемах с используемым на сервере сертификатом.
815	Сервер неожиданно прервал соединение	Возможно, в работе сервера произошел сбой	Попробуйте установить соединение позднее
816	Нет доверия к сертификату сервера	Отсутствует или неверный корневой сертификат	Корневой сертификта УЦ отсутствует, поврежден или находится не там, где нужно. Скопируйте корректный корневой сертификат УЦ на носитель, содержащий КриптоТуннель, в каталог crypto.

Код ошибки	Ошибка	Причина	Действия оператора
817	Сервер не отвечает	Возможно, сервер неработоспособен, доступ к нему заблокирован или есть ошибка в файле конфигурации	Проверьте, что компьютер подключен к Интернету. Если проблема сохранилась, проверьте, правильно ли отредактирован конфигурационный файл *stunnel.conf* (см. раздел 5) и при необходимости внесите исправления.
818	Сервер отвечает, но соединение с ним установить не удается	Возможно, настройки сервера не соответствуют настройкам клиента КриптоТуннель	Запросите у администратора сервера, какие настройки TLS-соединения он использует, отредактируйте соответствующим образом конфигурационный файл *stunnel.conf* (см. раздел 5)
819	Не удалось инициализировать ДСЧ	Возможно, существует проблема с файлом seed	Проверьте наличие и доступность на запись файла seed (расположен в папке программы).
821	Ваш сертификат отозван	Сертификат, с помощью которого Вы аутентифицируетесь на сервере, отозван	Выясните у администратора удостоверяющего центра причину отзыва и попросите у него создать для вас новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий КриптоТуннель, в каталог crypto.
823	Срок действия Вашего сертификата истек	У сертификата, с помощью которого Вы аутентифицируетесь на сервере, истек срок действия	Попросите администратора удостоверяющего центра создать для вас новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий КриптоТуннель, в каталог crypto.
825	Возможно, сервер требует клиентской аутентификации, а в КриптоТуннель не указан сертификат клиента	Сервер требует клиентской аутентификации	Внесите исправления в конфигурационный файл stunnel.conf, как описано в разделе 5.

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

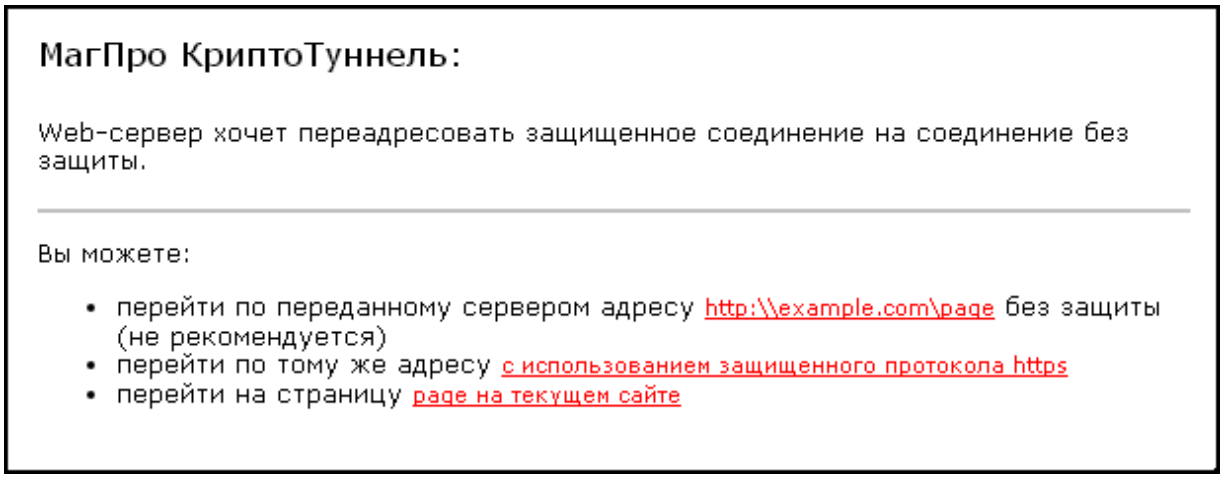
Код ошибки	Ошибка	Причина	Действия оператора
826	Сервер не принимает сертификат клиента как доверенный	Возможно, файл сертификатов клиента содержит не всю цепочку доверия, либо сервер не доверяет корневому сертификату.	Выясните у администратора сервера, есть ли на сервере корневой сертификат того удостоверяющего центра, на котором подписан пользовательский сертификат. Если такой корневой сертификат отсутствует, получите его у администратора удостоверяющего центра и попросите администратора сервера установить его. Если нужный корневой сертификат имеется, скорее всего пользовательский сертификат поврежден или отозван. Попросите у администратора сервера создать для вас новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий КриптоТуннель, в каталог crypto.

Код ошибки	Ошибка	Причина	Действия оператора
831	Сервер не смог проверить сертификат клиента.	Неподдерживаемый тип сертификата	Выясните у администратора сервера, есть ли на сервере корневой сертификат того удостоверяющего центра, на котором подписан пользовательский сертификат. Если такой корневой сертификат отсутствует, получите его у администратора удостоверяющего центра и попросите администратора сервера установить его. Если нужный корневой сертификат имеется, скорее всего пользовательский сертификат поврежден. Попросите у администратора удостоверяющего центра создать для пользователя новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий КриптоТуннель, в каталог crypto.
832	Сервер не смог проверить сертификат клиента.	Сертификат поврежден или же срок его действия еще не наступил	Попросите у администратора УЦ создать для вас новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий «КриптоТуннель» , в каталог crypto.

Код ошибки	Ошибка	Причина	Действия оператора
833	Сервер не смог проверить сертификат клиента.	Сообщение сервера: неизвестная ошибка при обработке сертификата клиента	Выясните у администратора сервера, почему сертификат клиента не удается проверить (возможно, он некорректен). Если администратор сервера не знает причину, или если сертификат некорректен, попросите у администратора УЦ создать для вас новый закрытый ключ и сертификат. Скопируйте их на носитель, содержащий КриптоТуннель, в каталог crypto.

7.3 Предупреждение о переходе по ссылке

При использовании опции *patch_location* возможно появление сообщения вида:



Данное сообщение «КриптоТуннель» выводит в случае обнаружения попытки переадресации защищенного соединения на соединение без защиты.

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

8 Приложения

8.1 Файлы сертификатов

8.1.1 Файл сертификатов УЦ

Для работы «МагПро КриптоПакет» в. 4.0 необходим файл, содержащий сертификаты удостоверяющих центров, на которых подписаны сертификаты серверов, с которыми устанавливается защищенное соединение. Имя этого файла указывается в качестве значения параметра CAfile в конфигурационном файле stunnel.conf (в приведенном выше примере это файл ca.crt).

Сертификаты в этом файле должны быть в формате PEM. Если сертификат УЦ получен в формате DER (расширения .cer или .crt) или PKCS#7 (расширение p7b), то для конвертации его в формат PEM можно воспользоваться утилитой openssl.

8.1.2 Ограничение на самоподписанные сертификаты серверов

Внимание. Если сертификат сервера является самоподписанным, то с помощью «МагПро КриптоПакет» в. 4.0 защищенное соединение с таким сервером установить нельзя. При попытке установить соединение с таким сервером пользователю будет выдано сообщение об ошибке.

8.1.3 Файл сертификатов и закрытый ключ пользователя

Если сервер требует клиентской аутентификации, у каждого пользователя должен быть файл сертификата, содержащий открытый ключ, и файл закрытого ключа, эти файлы можно получить в удостоверяющем центре или создать самостоятельно с помощью средства easy-gost, входящего в комплект поставки «МагПро КриптоПакет» в. 4.0. В конфигурационный файл stunnel.conf необходимо добавить параметры клиентской аутентификации, как описано в разделе 5.

8.2 Адреса страниц, приводящие к разрыву https-соединения

Когда пользователь, установив защищенное соединение с сервером с помощью «МагПро КриптоПакет» в. 4.0, переходит по внутренним ссылкам на другие страницы на этом сервере, в большинстве случаев переход осуществляется нормально и соединение остается защищенным. Но в некоторых случаях происходит переход к незащищенному соединению. Это связано с форматом, в котором во внутренних ссылках на сервере указаны адреса страниц, на которые переходит пользователь.

8.2.1 Абсолютные адреса

Если после установления HTTPS-соединения происходит переход на страницу, адрес которой на сайте сервера указан как относительный, HTTPS-соединение не разрывается. Но если адрес страницы указан как абсолютный (вида http(s)://[адрес]), то происходит попытка установить новое соединение напрямую. Если адрес страницы имеет вид http://[адрес], то соединение устанавливается, но уже незащищенное, и пользователь может этого вообще не заметить. Если адрес страницы имеет вид https://[адрес], то соединение установить, скорее всего, не удастся, т.к. сам браузер не может работать с алгоритмами ГОСТ, и пользователь

получит сообщение об ошибке. Поэтому все ссылки на защищаемом сайте должны быть относительными.

8.2.2 Использование Redirection

В ответ на запросы клиента web-сервер может вернуть код 3xx (Redirection/перенаправление), этот ответ предписывает браузеру перейти по ссылке, указанной в заголовке Location. При включенной опци *patch_location* такое перенаправление в большинстве случаев отработает правильно, однако следует иметь ввиду, что переадресация на другой порт того же сервера не поддерживается.

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

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