КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-04 34 07 - ЛУ

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

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» в. 3.0

Средство защиты доступа к сетевым ресурсам «КриптоТуннель»

Руководство по использованию

СЕИУ.00009-04 34 07
Листов 45

Литера О

2019

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. 3.0.

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. 3.0 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, FTP (passive mode), NFS, SQL и т.д.

Наиболее востребованным применением «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» является защита соединений с веб-серверами.

Отличительной особенностью «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» является возможность защитить соединения без существенного изменения настроек прикладного ПО.

«КриптоТуннель» — это составная часть СКЗИ «МагПро КриптоПакет» в. 3.0, 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

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» 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.

3 Перечень функций

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» реализует защиту канала по протоколу 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.

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

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» в. 3.0

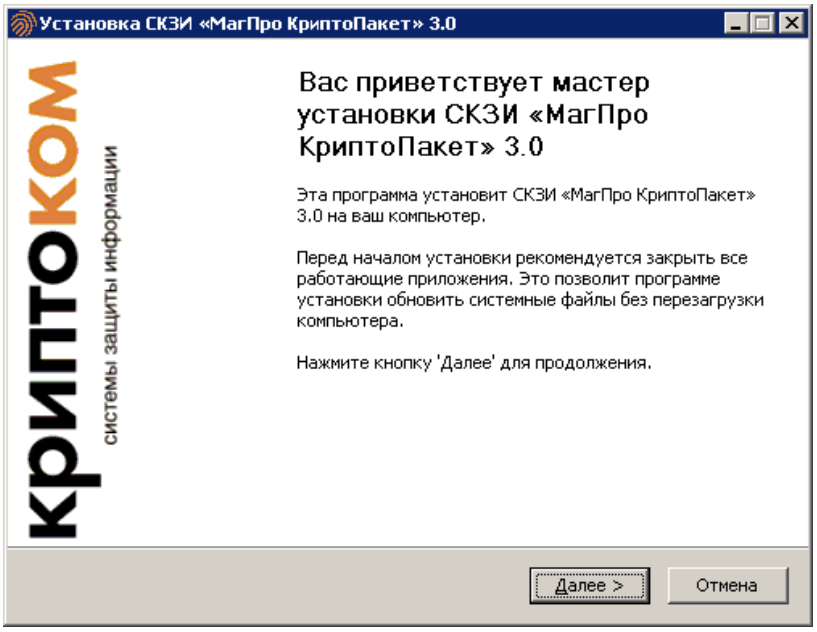
Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» в. 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» в. 3.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Правила пользования» (СЕИУ.СЕИУ.00009–04 94).

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

5 Установка

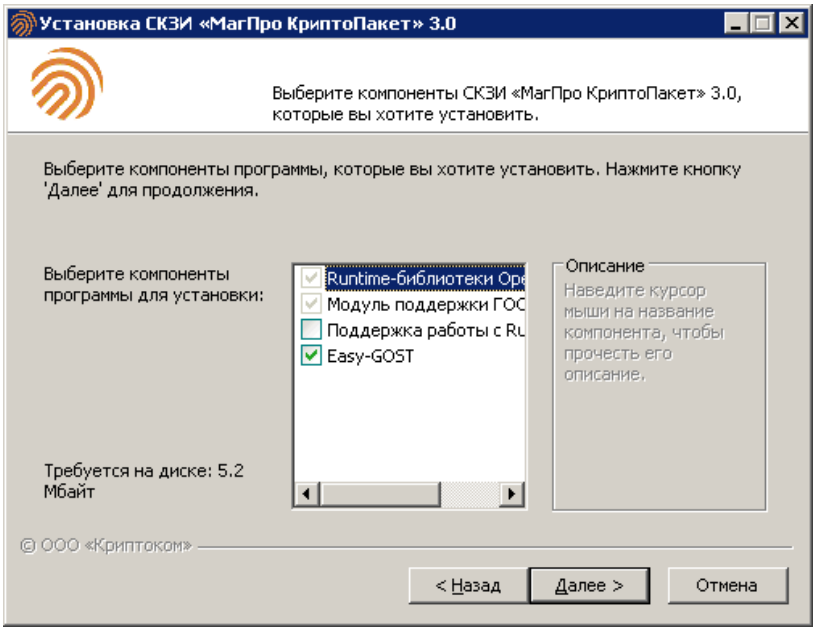
5.1 Установка серверной части для ОС семейства Windows

1. Запустить пакет инсталляции mpcp3base-<номер_сборки>-<разрядность>-standard. Если «МагПро КриптоПакет» в. 3.0 уже установлен, перейти к пункту 9.



Нажать на кнопку «Далее».

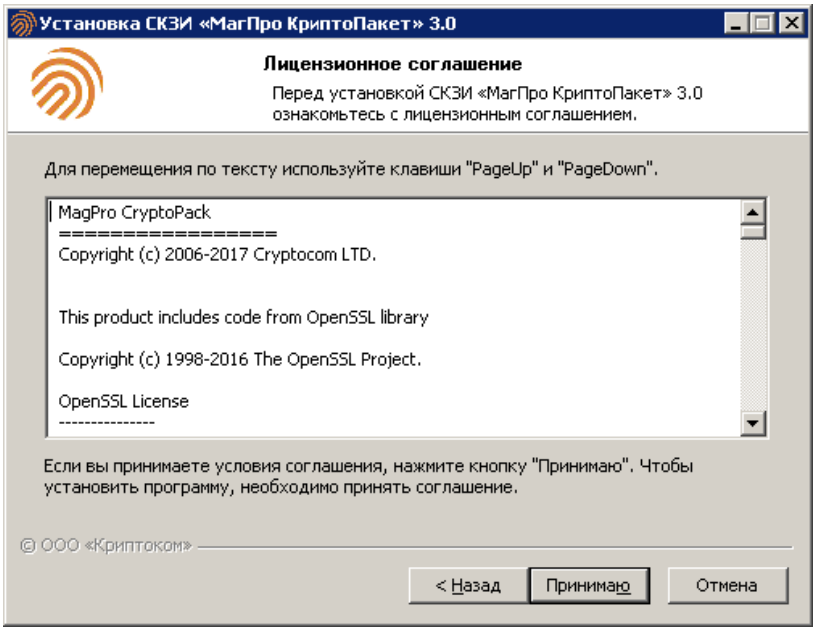
2. Выводится окно выбора компонентов программы.



Выбрать необходимые компоненты и нажать на кнопку «Далее».

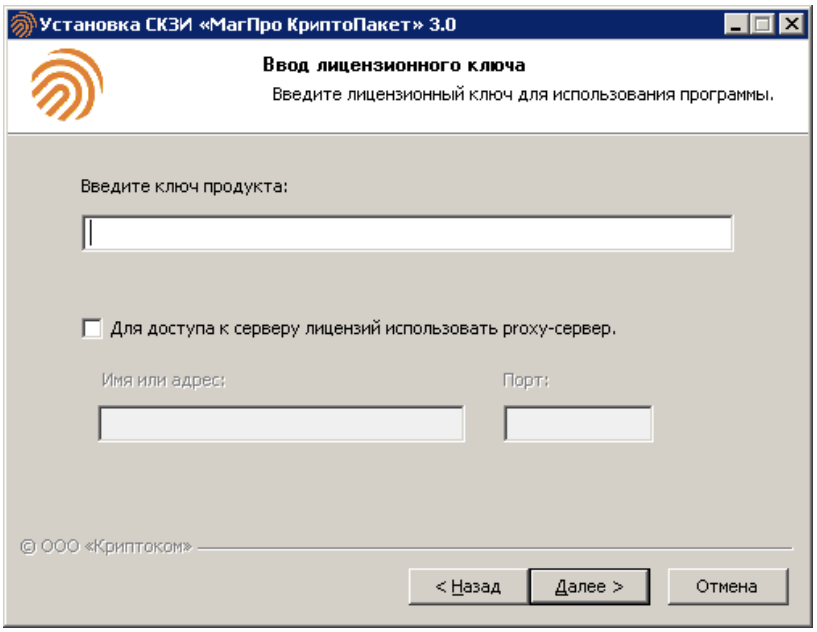
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Выводится окно лицензионного соглашения:



Прочесть его. При согласии нажать на кнопку «Принимаю».

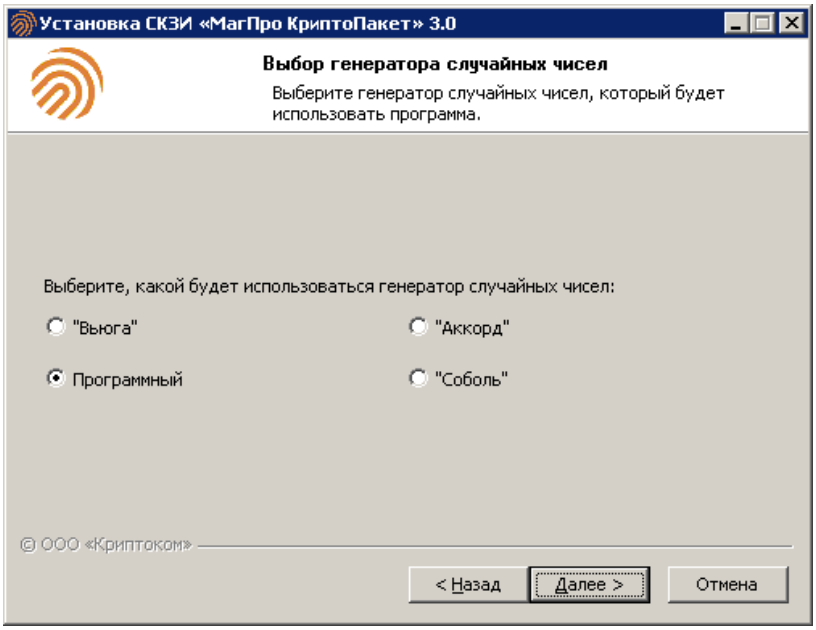
4. Выводится окно ввода лицензионного ключа продукта.



Ввести лицензионный ключ продукта. Если для доступа к серверу лицензий предполагается использовать proxy-сервер, выбрать соответствующую опцию в окне и указать адрес и порт сервера. Нажать на кнопку «Далее».

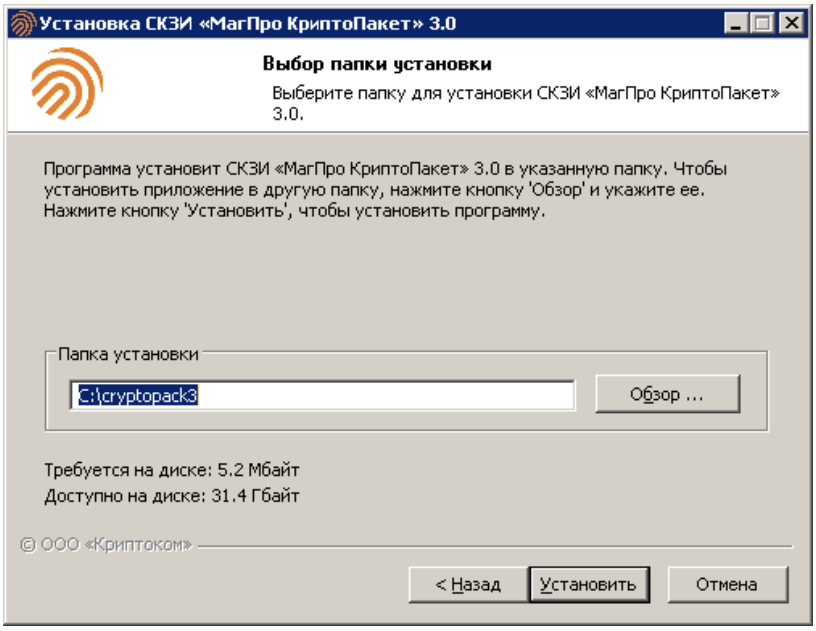
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5. Выводится окно выбора генератора случайных чисел.



Выбрать используемый генератор. Нажать на кнопку «Далее».

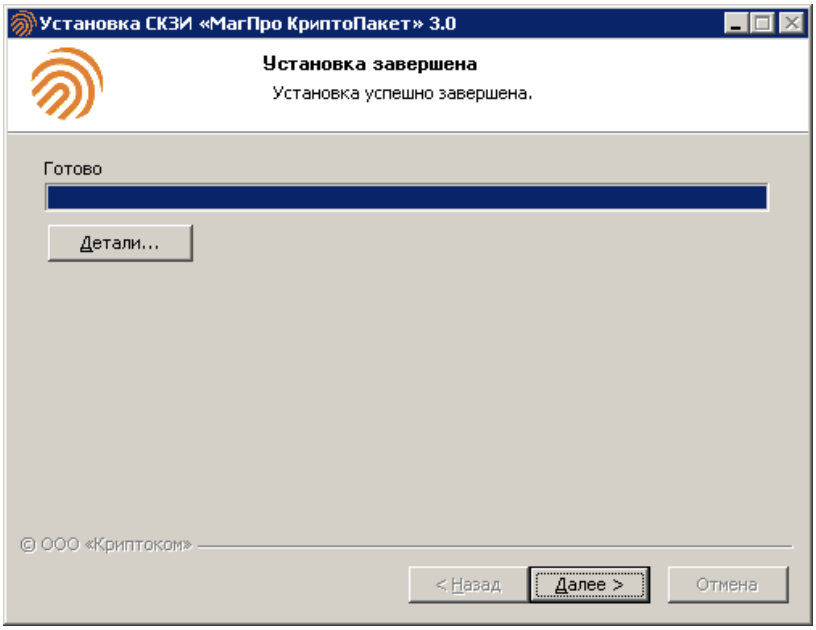
6. Выводится окно выбора папки установки.



В случае необходимости изменить папку установки, используемую по умолчанию. Нажать на кнопку «Установить».

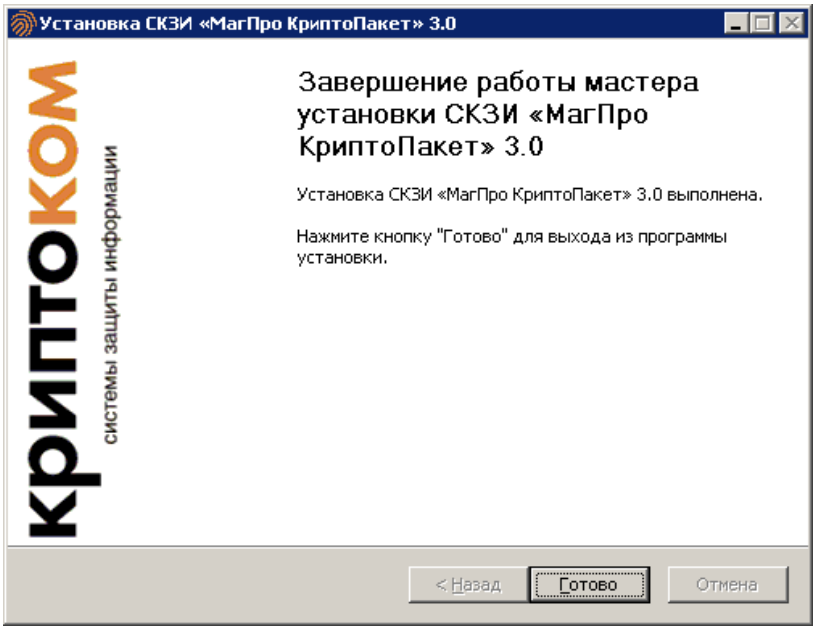
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7. Выводится окно, отражающее процесс установки:



После завершения процесса установки нажать на кнопку «Далее».

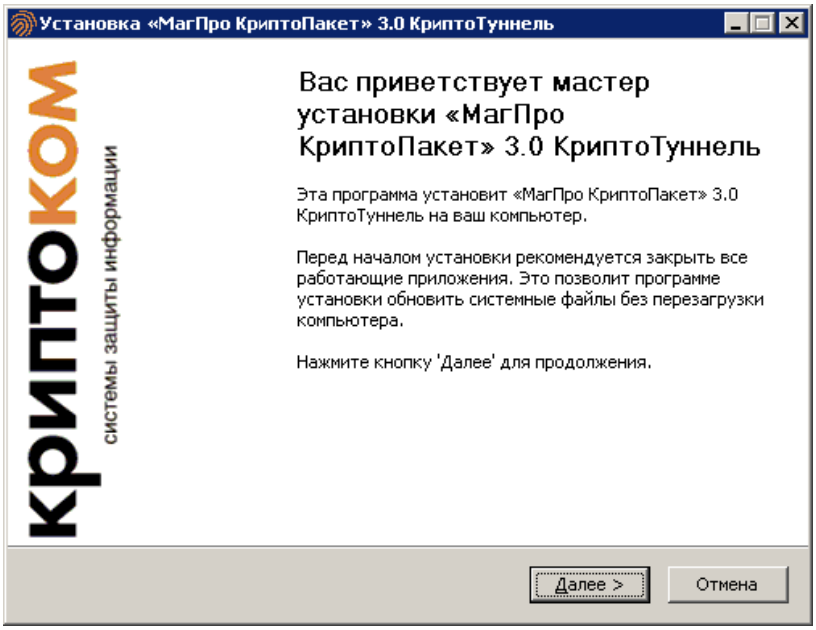
8. Выводится окно с сообщением об окончании установки «МагПро КриптоПакет» в. 3.0:



Нажать на кнопку «Готово».

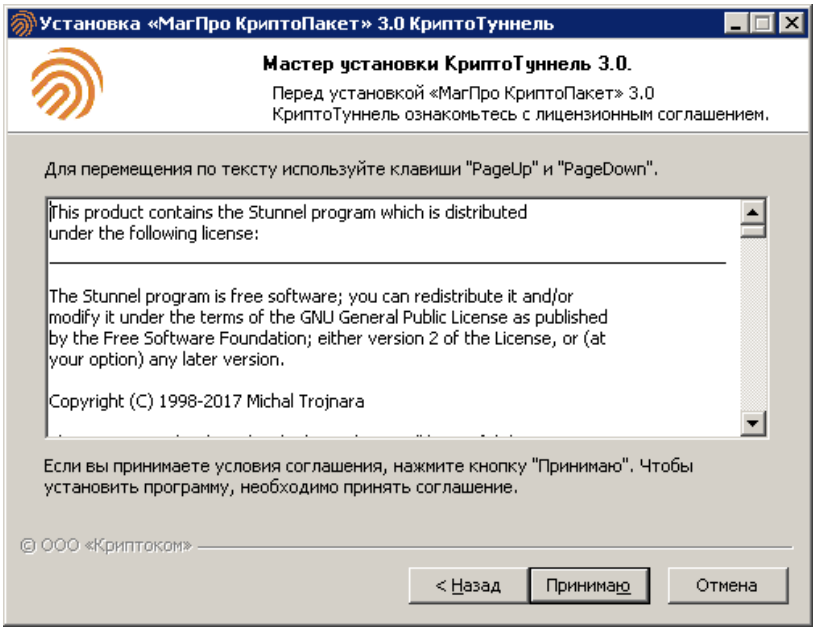
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

9. Запустить пакет инсталляции mpcp3ct-server-<номерi_сборки>-<разрядность>.



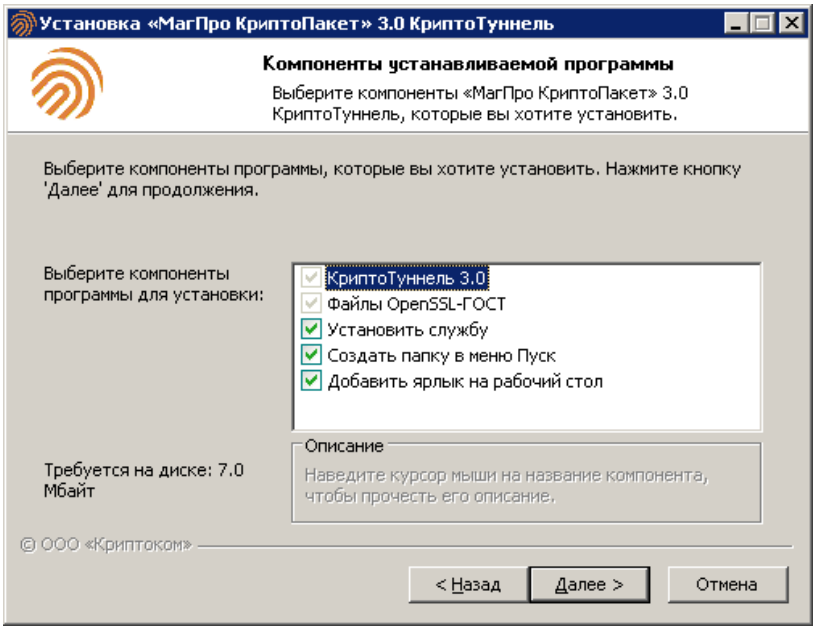
Нажать на кнопку «Далее».

10. Выводится окно лицензионного соглашения. Прочесть его и при согласии нажать на кнопку «Принимаю»:



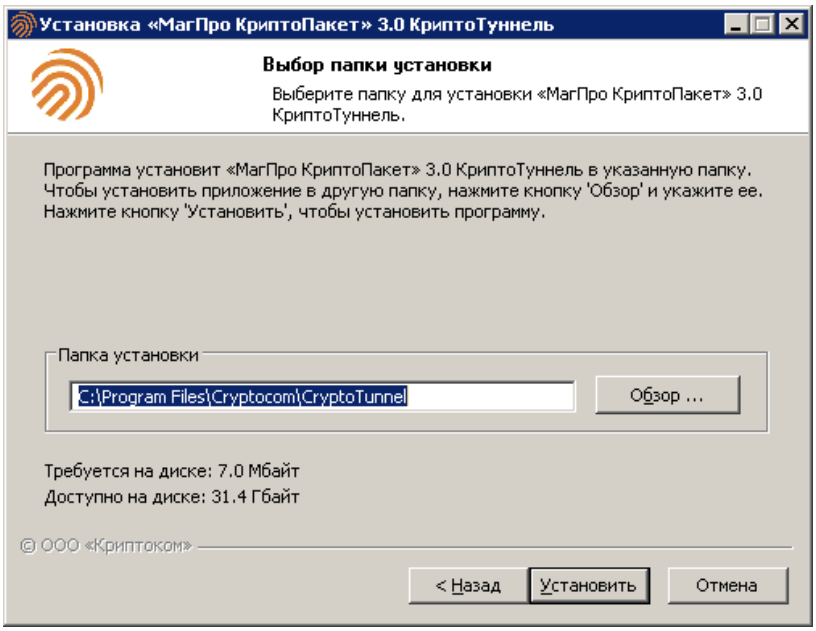
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

11. Выводится окно выбора компонентов программы.



Выбрать необходимые компоненты. При этом следует учитывать, что КриптоТуннель может работать не только как приложение, но и как служба. Если нет необходимости запуска КриптоТуннеля как службы, рекомендуется снять флаг напротив компонента «**Установить службу**». В противном случае выбор этого компонента обязателен.
Нажать на кнопку «Далее».

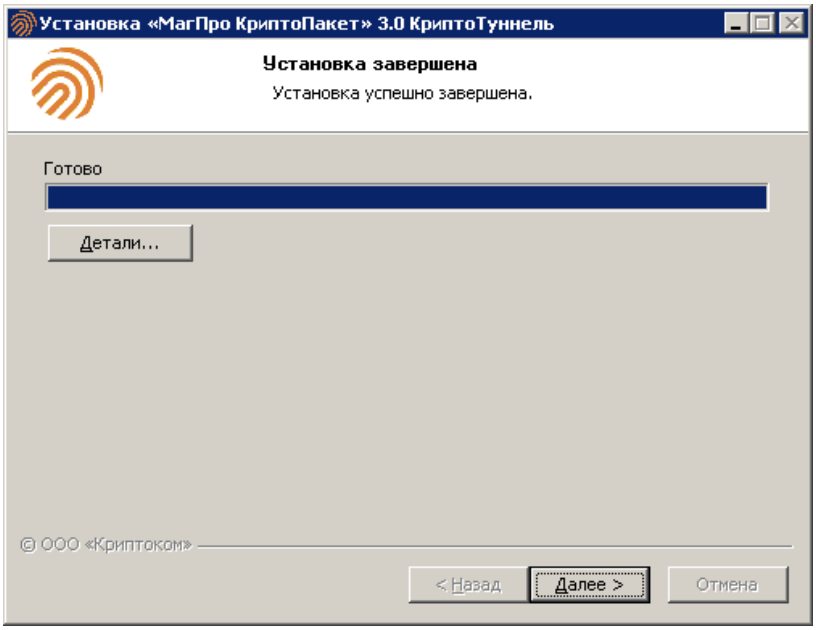
12. Выводится окно выбора папки установки.



В случае необходимости изменить папку установки, используемую по умолчанию. Нажать на кнопку «Установить».

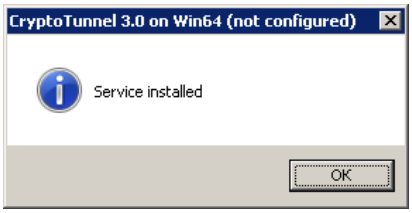
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

13. Выводится окно, отражающее процесс установки:



После завершения процесса установки нажать на кнопку «Далее».

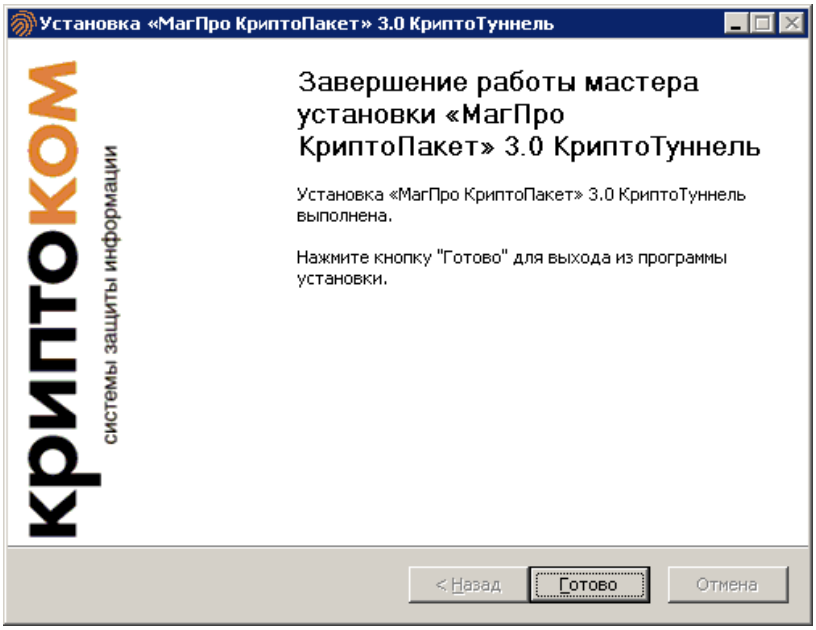
14. Если при выборе компонентов программы был установлен флаг **«Установить службу»**, то во время установки выводится окно, сообщающее об успешной установке службы:



Нажать кнопку «Ок».

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

15. Выводится окно с сообщением об окончании установки «МагПро КриптоПакет» в. 3.0:



Нажать на кнопку «Готово».

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

5.2 Установка клиентской части для ОС семейства Windows

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» может устанавливаться как на жесткий диск компьютера, так и на подключаемые носители (флеш-диски). Установка программного комплекса заключается в копировании на диск файлов, входящих в состав программного комплекса (подкаталог CryptoTunnel дистрибутива).

В состав программного комплекса входят:

– Программа stunnel и вспомогательные модули

```
stunnel.exe
starter.exe
USB_Disk_Eject.exe
```

– Базовые компоненты «МагПро КриптоПакет» в. 3.0 и модули работы с криптографическими ключами

```
libeay32.dll
ssleay32.dll
cryptocom.dll
openssl.exe
openssl.cnf
mkkey.exe
mkseed.exe
updater.exe
vars.bat
```

– Модули поддержки устройства Рутокен

```
ce_rutoken_keys.dll
opensc.dll
rt-key-util.exe
```

– конфигурационные файлы

```
stunnel.conf
starter.ini
```

5.3 Установка для UNIX-подобных ОС

Для установки «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» :

1. Перейдите в каталог с установочными файлами (пакетами).
2. С помощью системных утилит (dpkg, apt, rpm, yum, dnf и т.д.) установите пакеты

```
openssl-r*
stunnel-gost*
```

подходящей архитектуры. Возникающие зависимости следует разрешать с помощью системного или иного репозитория, которому Вы доверяете. Установка производится в каталог /opt.

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

6 Настройка

6.1 Настройка сервера

В данном разделе описывается настройка «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» на стороне сервера. «КриптоТуннель» в этом случае 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. Проверить и при необходимости изменить параметры общей секции конфигурационного файла *stunnel.conf*. Как правило, данная секция не требует редактирования. Типовой вид:

```
engine = cryptocom
engineDefault = ALL
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
```

   Подпробное описание опций общей секции см. в разделе 6.3.

2. Добавить 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
ciphers = GOST2012-GOST8912-GOST8912
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 6.3.

3. Выполнить формирование ключевой инфраструктуры в соответствии с описанием в разделе 6.5. Сформированные файлы расположить в соответствии с параметрами, указанными в *stunnel.conf*.

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

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

Для ОС семейства Linux/Unix: выполнить перезапуск stunnel.

5. Правильно настроить и запустить защищаемое приложение.

6.2 Настройка клиента

В данном разделе описывается настройка «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» на стороне клиента. «КриптоТуннель» в этом случае 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 и при необходимости изменить параметры общей секции конфигурационного файла *stunnel.conf*. Как правило, данная секция не требует редактирования. Типовой вид:

```
client = yes
engine = cryptocom
engineDefault = ALL
engineCtrl = RNG:PROGRAM
engineCtrl = RNG_PARAMS:seed
```

   Подпробное описание опций общей секции см. в разделе 6.3.

2. Добавить секцию настройки удалённого подключения.
   Типовой вид:

```
[someserver.ru]
protocol = http
accept = 8080
connect = tls.someserver.ru:443
ciphers = GOST2012-GOST8912-GOST8912
CAFile = .\crypto\ca.crt
TIMEOUTclose = 0
```

   Название секции выбирается произвольно. Рекомендуется устанавливать наиболее удобное для чтения журнала значение.
   Для настройки работы через прокси-сервер необходимо изменить строки секции следующим образом:

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

   При необходимости указать дополнительные опции подключения к прокси-серверу, такие как *protocolAuthentication, protocolDomain, protocolUsername и protocolPassword*.
   Подпробное описание опций см. в разделе 6.3.

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

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:

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

   Описание ключевой инфраструктуры см. в разделе 6.5.

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 6.4.

6.3 Конфигурационный файл *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.

6.3.1 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 = cryptocom
используемый энжин

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

engineCtrl = COMMAND [: PARAMETER]
управление энжином

Служит для настройки энжина. Для энжина cryptocom при настройке ДСЧ могут быть использованы следующие настройки:

```
engineCtrl = RNG:PROGRAM
engineCtrl = RNG_PARAMS:seed
```

engineDefault = TASK_LIST
список задач энжина

Задаёт задачи, делегированные указанному энжину. Могут быть выбраны следующие задачи:
ALL, RAND, CIPHERS, DIGESTS, PKEY, PKEY_CRYPTO, PKEY_ASN1.

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.

6.3.2 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

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

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

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

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

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

определяет набор используемых шифров TLS-соединения

В большинстве случаев следует указывать GOST2012-GOST8912-GOST8912.

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.

engineNum = ENGINE_NUMBER

задаёт используемый энжин по номеру

Энжины нумеруются, начиная с 1. Т.к. «МагПро КриптоПакет» в. 3.0 допускает использование только одного энжина (cryptocom), для этой опции следует всегда использовать значение 1. Данная опция может потребоваться в случае использования аппаратных решений аутентификации (например, для ключей, хранящихся на RuToken).

key = KEY_FILE

закрытый ключ сертификата, указанного в опции cert

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).

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)*.

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

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)*.

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 во время установления соединения по указанному протоколу.
Используется только на стороне клиента протоколом *connect*.

protocolHost = HOST:PORT
адрес подключения

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

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*.

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.

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*.

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.

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

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

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

sslVersion = SSL_VERSION

версия TLS протокола

Поддерживаются версии TLSv1, TLSv1.1, TLSv1.2

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

TIMEOUTclose = SECONDS
время ожидания close_notify

Рекомендуется устанавливать это значение в 0.

TIMEOUTconnect = SECONDS
время ожидания соединения с удалённым хостом

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

6.3.3 Настройка HTTP параметров защищённых соединений

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

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

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.

6.4 Конфигурационный файл *starter.ini*

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

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

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

6.4.1 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.

6.4.2 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

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. 3.0 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.

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

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.

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.

6.4.3 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 7.1.2).

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.

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

6.5 Ключевая инфраструктура

6.5.1 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 6.3.2.
2. Сертификат сервера должен содержать расширение Enhanced Key Usage со значением *Server Authentication (1.3.6.1.5.5.7.3.1)*.

6.5.2 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)*.

6.5.3 Формат файлов ключевой информации

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

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

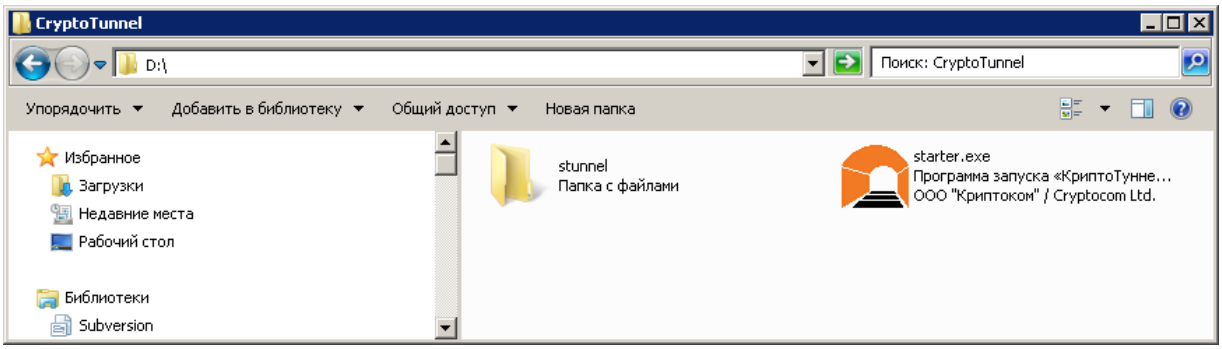
7 Использование

7.1 Использование в ОС семейства Windows

7.1.1 Запуск «МагПро КриптоПакет» в. 3.0 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. 3.0 в исполнении «КриптоТуннель» :



3. Запустить «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» , дважды щелкнув мышью по иконке starter.

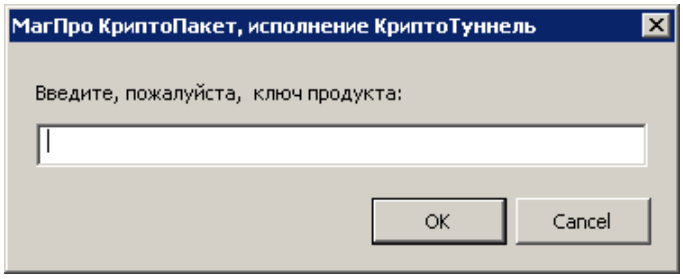
Если закрытый ключ сервера/пользователя, указанный в конфигурационном файле *stunnel.conf*, защищен PIN-кодом, то после запуска «КриптоТуннель» появится окно запроса PIN-кода ключа:

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

7.1.2 Лицензирование

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

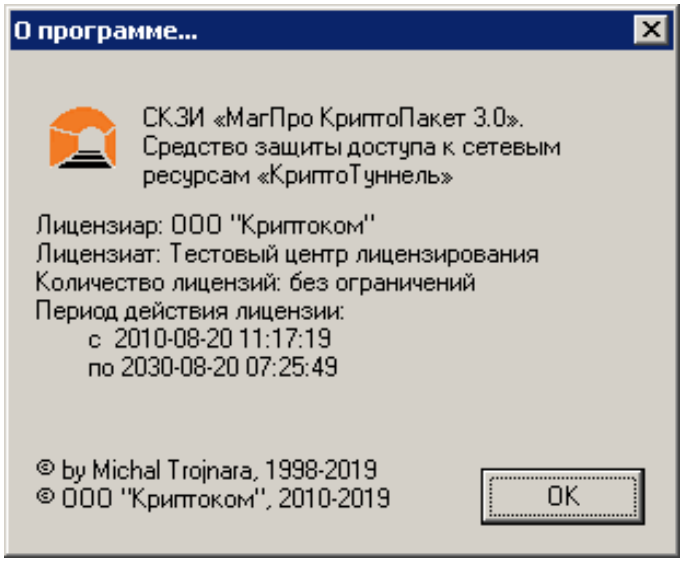


От оператора требуется ввести ключ продукта и нажать кнопку «OK».

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, 7) 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.

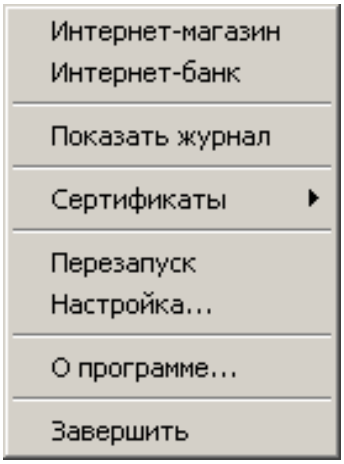
Для просмотра сведений о текущей лицензии необходимо выбрать пункт «О программе...» контекстного меню. В этом случае откроется окно, содержащее сведения о продукте и лицензии:



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

7.1.3 Контекстное меню

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



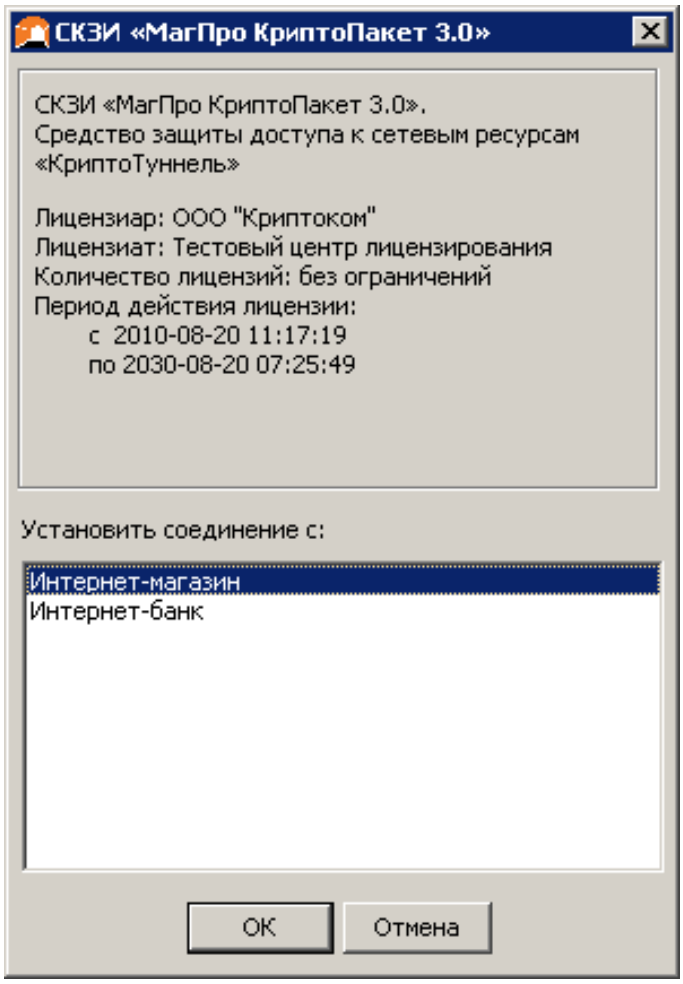
Контекстное меню состоит из двух частей. В верхней части выводится список алиасов http-страниц, на которые можно перейти после установления защищённого соединения (см. 6.4.2). В нижней части выводятся служебные пункты:

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

7.1.4 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. 3.0 в исполнении «КриптоТуннель» продолжит работу, иконка в трее остается.

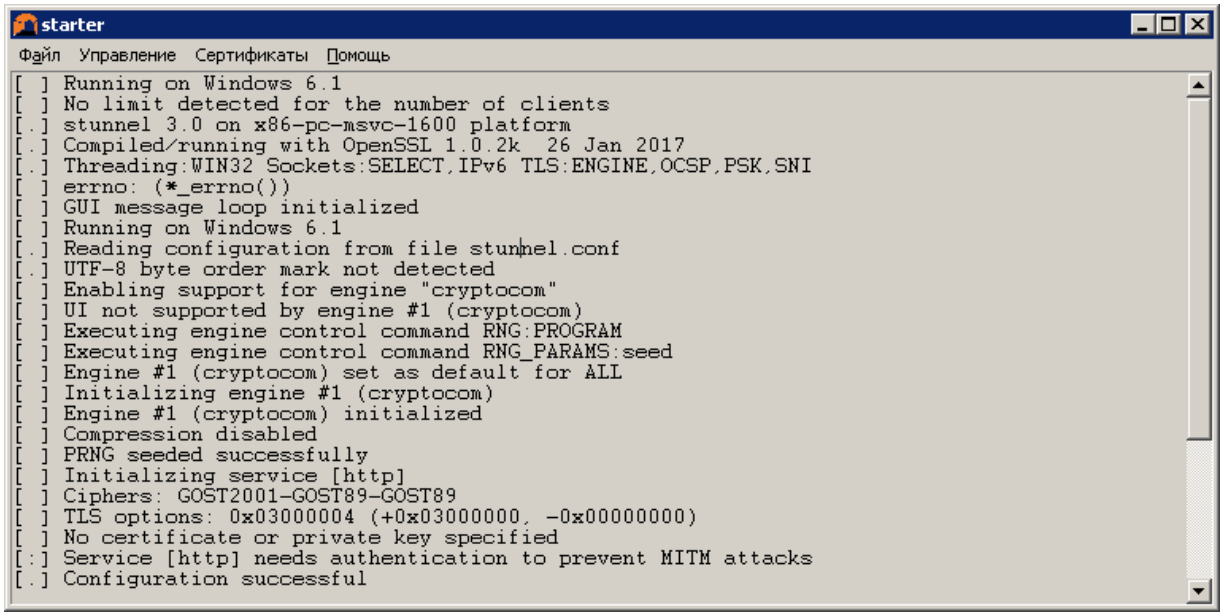
Помимо описанных выше способов, перейти на нужную страницу можно через контекстное меню, щёлкнув правой кнопкой мыши по иконке «МагПро КриптоПакет» в. 3.0 в трее. В контекстном меню в верхней его части будут содержаться пункты, названия которых соответствуют алиасам страниц, указанных в секции *urls* файла *starter.ini*. Для перехода на нужную страницу следует щелкнуть левой кнопкой мыши по соответствующему пункту.

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

7.1.5 Журнал работы «КриптоТуннель»

Журнал работы «МагПро КриптоПакет» в. 3.0 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» .

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 6.3).

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

7.1.6 Выход из программы

Выход из программы осуществляется только через контекстное меню. Для этого необходимо в меню найти пункт «Завершить» и щёлкнуть по нему левой кнопкой мыши.

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.

7.1.7 Служба «КриптоТуннель»

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

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

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*.

7.2 Использование в UNIX-подобных ОС

В случае использования программного датчика случайных чисел перед первым запуском «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» необходимо создать файл инициализации программного ДСЧ. Для этого необходимо запустить программу

```
sudo -H /opt/cryptopack3/bin/mkseed -r
```

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 6, «КриптоТуннель» готов к работе. Запуск осуществляется командой

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

или

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

в зависимости от типа ОС,

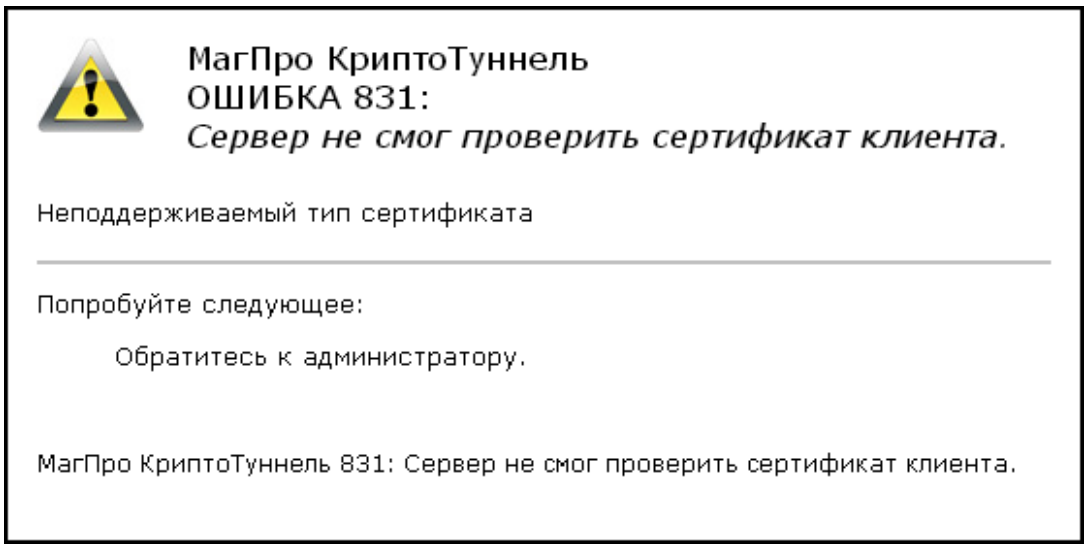
Если во время запуска «КриптоТуннель» возникают ошибки, связанные с неверной конфигурацией, то будет сформирован специальный лог-файл *stunnel.start.log*, включающий соответствующие сообщения. Сообщения о прочих ошибках, возникающих при работе «КриптоТуннель» , добавляются в основной журнал (задаётся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

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*.

8 Сообщения оператору

8.1 Общие замечания

Если при работе «МагПро КриптоПакет» в. 3.0 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.

8.2 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 6) 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 6) 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 6)
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 6.

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

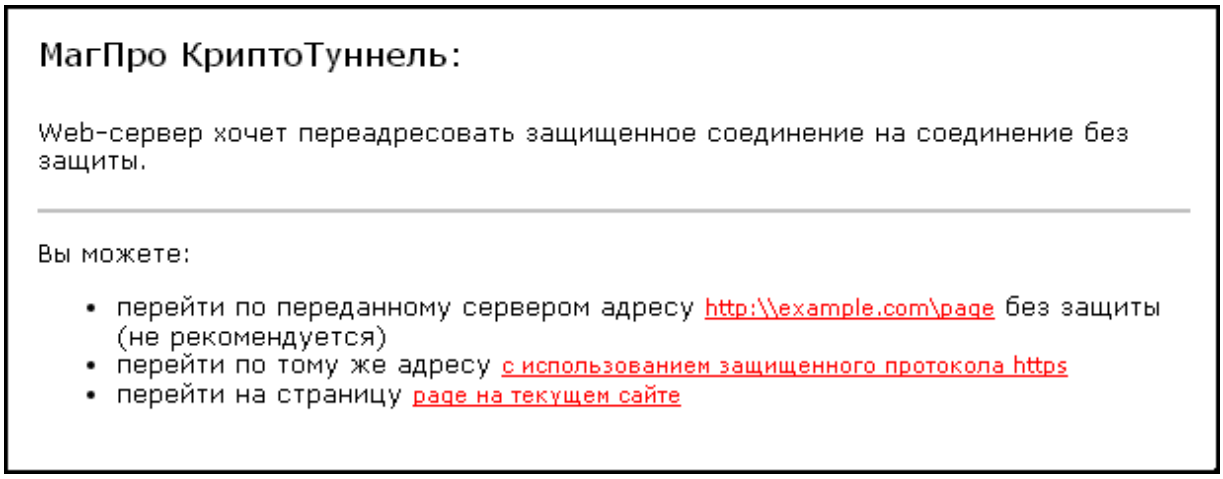
Код ошибки	Ошибка	Причина	Действия оператора
826	Сервер не принимает сертификат клиента как доверенный	Возможно, файл сертификатов клиента содержит не всю цепочку доверия, либо сервер не доверяет корневому сертификату.	Выясните у администратора сервера, есть ли на сервере корневой сертификат того удостоверяющего 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.

8.3 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

9 Приложения

9.1 Файлы сертификатов

9.1.1 Файл сертификатов УЦ

Для работы «МагПро КриптоПакет» в. 3.0 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 PE Mможно воспользоваться утилитой openssl.

9.1.2 Ограничение на самоподписанные сертификаты серверов

Внимание. Если сертификат сервера является самоподписанным, то с помощью «МагПро КриптоПакет» в. 3.0 защищенное соединение с таким сервером установить нельзя. При попытке установить соединение с таким сервером пользователю будет выдано сообщение об ошибке.

9.1.3 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. 3.0 в исполнении «КриптоТуннель» . В конфигурационный файл stunnel.conf необходимо добавить параметры клиентской аутентификации, как описано в разделе 6.

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

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