КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-04 34 07 - ЛУ

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

2018

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» позволяет:

- установить соединение с web-сервером, защищенное по протоколу TLS (HTTPS-соединение), с использованием алгоритмов ГОСТ, не меняя содержания файлов, содержащихся на компьютере пользователя;
- установить защищенное RDP-соединение с удаленным компьютером;
- выработать электронную подпись под текстовыми данными или файлом, которые передаются пользователем через веб-форму;
- получить в службе временных меток метку времени для подписываемых данных.

«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 следующие функции:

- реализации протокола TLS с использованием российских наборов алгоритмов шифрования TLS_GOSTR341112_256_WITH_28147_CNT_IMIT и TLS_GOSTR341001_WITH_28147_CNT_IMIT
  (набор TLS_GOSTR341001_WITH_28147_CNT_IMIT следует использовать только для соединения с серверами, не поддерживающими набор TLS_GOSTR341112_256_WITH_28147_CNT_IMIT);
- создание и проверка электронной подписи в соответствии с ГОСТ Р 34.10 для файлов и данных, вводимых пользователем;
- получение метки времени в службе временных меток.

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

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

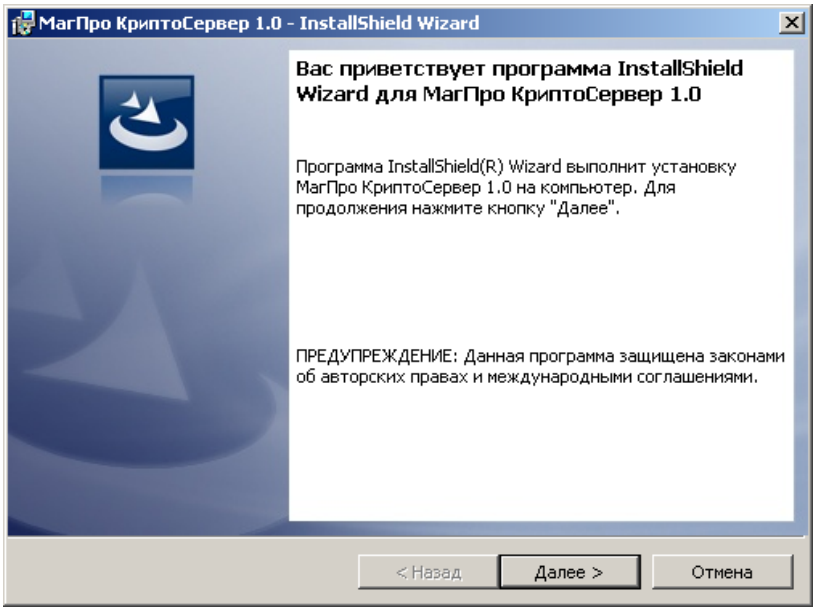
Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» в. 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» в. 3.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0.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

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

5 Установка

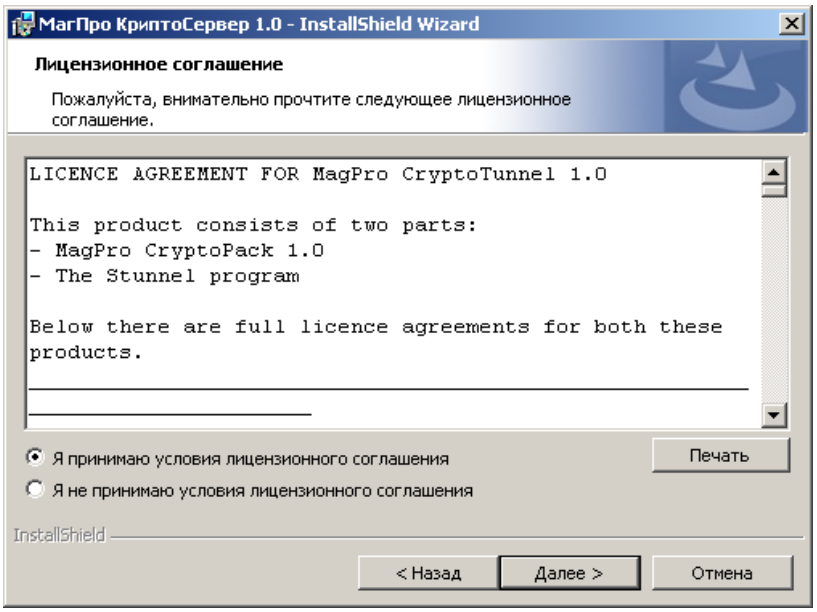
5.1 Установка серверной части для ОС семейства Windows

1. Запустить пакет инсталляции mpcp-3.0-cryptotunnel-server.



Нажать на кнопку «Далее».

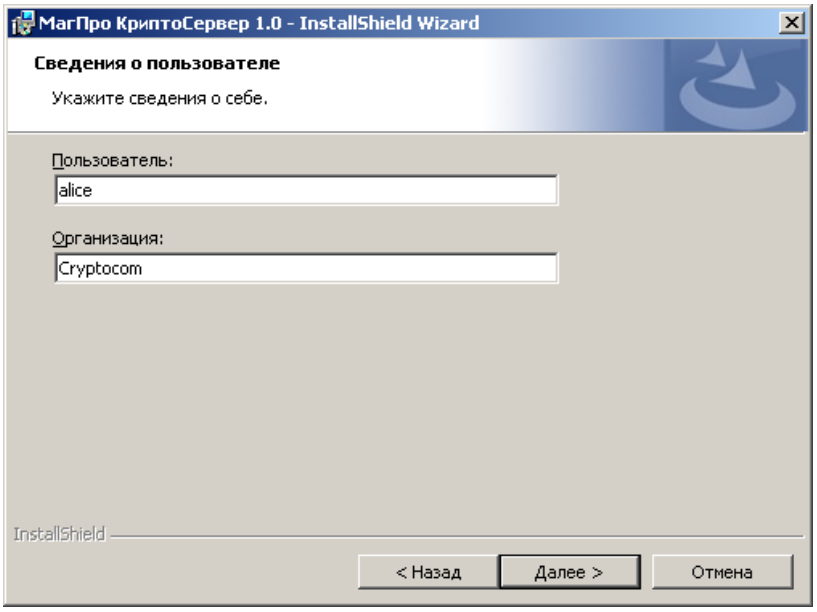
2. Выводится окно лицензионного соглашения. Прочесть его и при согласии выбрать «Я принимаю условия лицензионного соглашения»:



Нажать на кнопку «Далее».

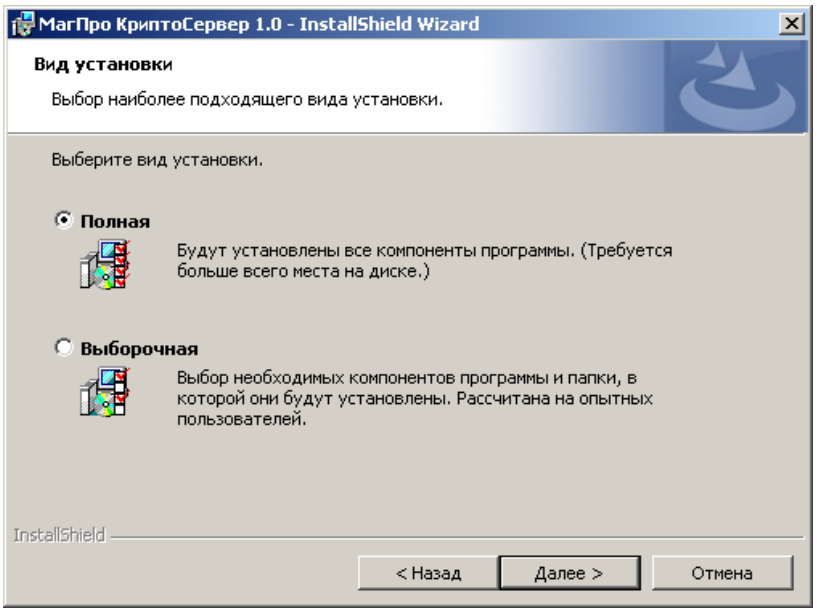
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Указать сведения о себе и об организации.



Нажать на кнопку «Далее».

4. Выводится окно выбора вида установки — полная или выборочная.

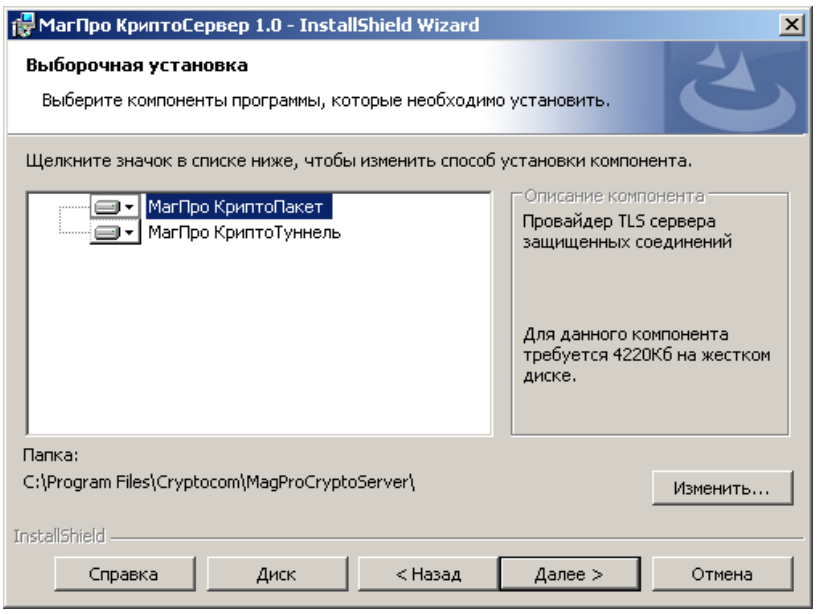


В «МагПро КриптоПакет» в. 3.0 нет компонентов, которые можно исключить из установки, но на странице выборочной установки можно изменить установочный каталог, заданный по умолчанию.

Выбрав вид установки, нажать на кнопку «Далее».

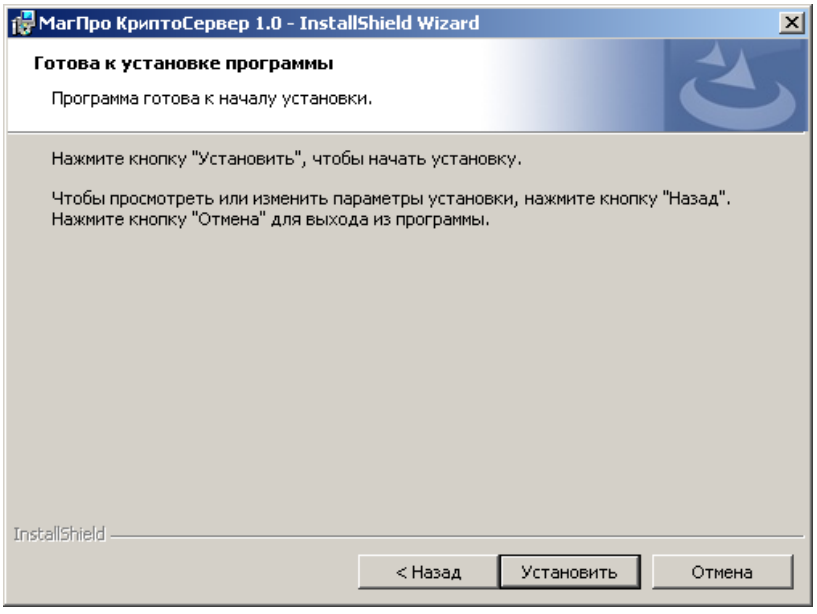
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5. Если на предыдущем шаге указана выборочная установка, выводится окно выбора компонентов:



Если необходимо, изменить установочный каталог, заданный по умолчанию, нажав на кнопку «Изменить».
Нажать на кнопку «Далее».

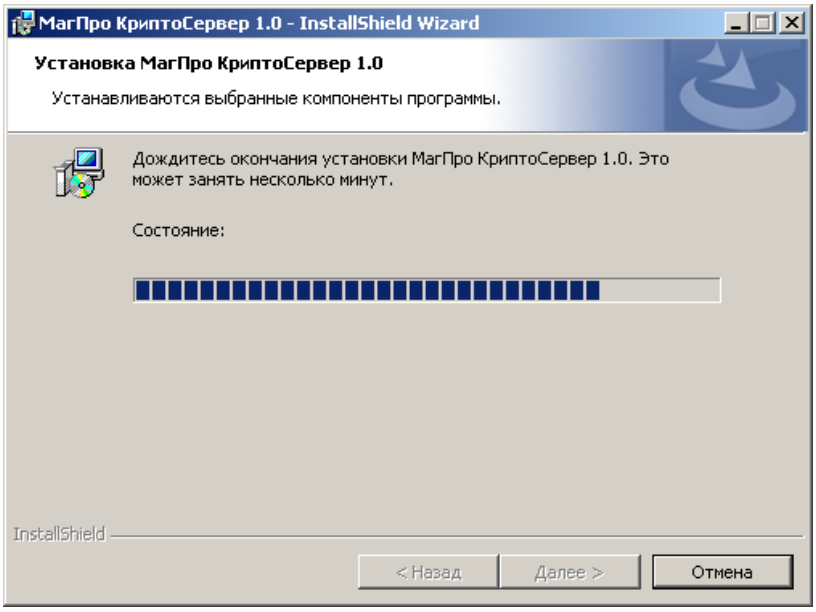
6. Выводится окно, сообщающее о готовности программы к установке.



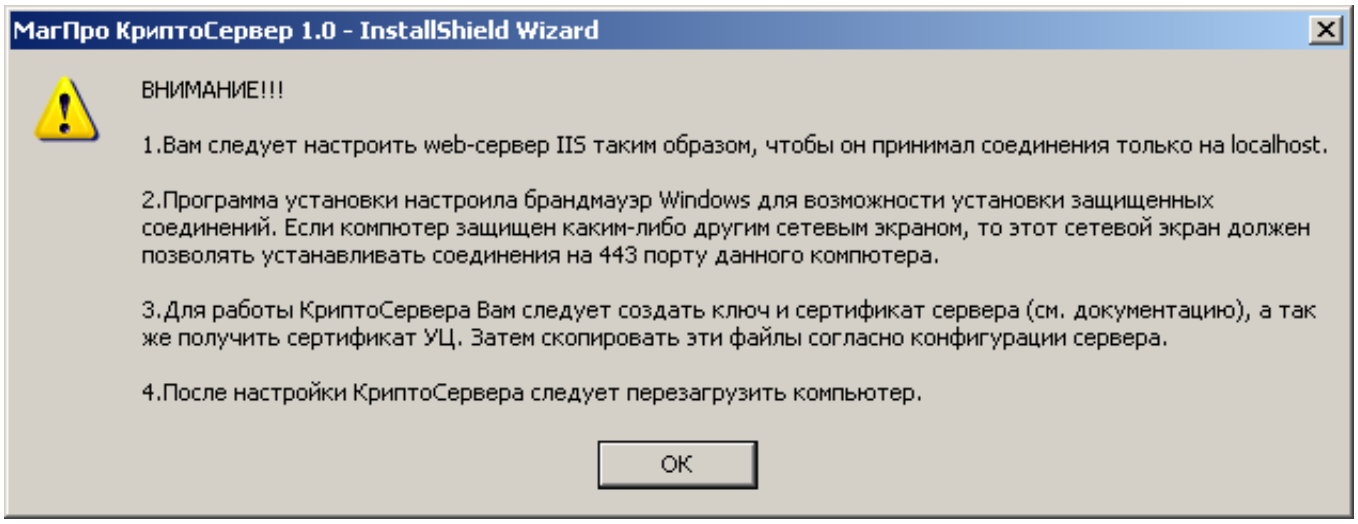
Нажать на кнопку «Далее».

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

7. Выводится окно, отражающее процесс установки:



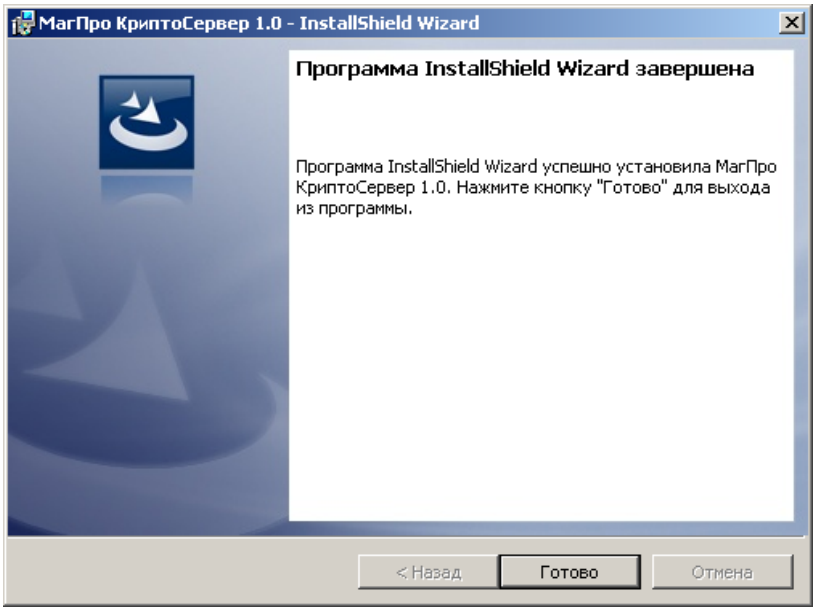
8. Во время установки выводится окно, содержащее важные предупреждения:



Для завершения установки необходимо нажать кнопку «Ок».

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

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



Нажать на кнопку «Готово».

5.2 Установка клиентской части для ОС семейства Windows

5.2.1 Состав

В состав программного комплекса входят:

– Программа stunnel и вспомогательные модули

```
stunnel.exe
curl.exe
USB_Disk_Eject.exe
```

– Необходимые компоненты «МагПро КриптоПакет» в. 3.0

```
libeay32.dll
ssleay32.dll
cryptocom.dll
updater.exe
```

– Программа запуска starter

```
starter.exe
```

– Файл сертификатов удостоверяющих центров в формате PEM
– Конфигурационные файлы

```
stunnel.conf
starter.cfg
urls
```

В состав комплекса могут также входить файл сертификата клиента и файл, содержащий закрытый ключ клиента, если сервер требует клиентской аутентификации или если используется электронная подпись.

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

5.2.2 Установка на подключаемые носители

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» устанавливается на подключаемые носители: flash-устройства и лазерные диски. Установка программного комплекса заключается в копировании файлов, входящих в состав программного комплекса в определённые каталоги носителя.

- В выбранный каталог носителя информации помещается файл starter.exe.
- В подкаталог stunnel помещаются файлы программы stunnel, файлы «МагПро КриптоПакет» в. 3.0, конфигурационные файлы.
- Положение остальных файлов определяется настройкой конфигурационного файла stunnel.conf.

5.2.3 Установка в каталог на стационарном носителе компьютера

Для установки программного комплекса «КриптоТуннель» на стационарный носитель компьютера пользователя, необходимо скопировать файлы, входящие в состав программного комплекса в выбранный подкаталог стационарного носителя компьютера.

- В выбранный каталог помещается файл starter.exe.
- В подкаталог stunnel помещаются файлы программы stunnel, файлы «МагПро КриптоПакет» в. 3.0, конфигурационные файлы.
- Положение остальных файлов определяется настройкой конфигурационного файла stunnel.conf.

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*
   ```

   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

6.1.1 Общие замечания

КриптоТуннель серверное исполнение предназначен для защиты соединения до некоего серверного приложения. Особенно можно выделить веб-сервер (протокол HTTP) и RDP-сервер (протокол RDP), однако возможна защита и других протоколов. Поскольку КриптоТуннель является отдельным приложением, он выступает фронт-эндом перед защищаемым бэк-энд приложением: он принимает зашифрованное TLS-соединение от клиентской части и после выполнения собственных криптографических операций передаёт расшифрованные данные защищаемому приложению. Таким образом он должен быть настроен на приём соединений из сети интернет на передачу в безопасную внутреннюю сеть.

Для настройки КриптоТуннеля нужно выполнить следующие действия:

1. Внести в файл конфигурации stunnel.conf необходимые изменения в соответствии с разделом 6.1.1.1.
2. Установить сертификат сервера, соответствующий ему закрытый ключ и корневой сертификат УЦ в соответствии с конфигурационным файлом stunnel.conf.
3. Для ОС семейства Windows сделать рестарт сервиса stunnel.
4. Правильно настроить и запустить защищаемое приложение.

6.1.1.1 Файл stunnel.conf

Файл stunnel.conf является конфигурационным файлом КриптоТуннель. Он содержит в себе общую секцию и может содержать в себе несколько секций для различных виртуальных хостов. Общая секция имеет обязательную часть в начале файла, ограниченную символами #, которая не требует изменений.

6.1.1.1.1 Настройки общей секции

Общая секция включает следующие опции:

output указывает на лог-файл приложения. В нем будет отображаться информация о подключениях пользователей и возможных ошибках.

debug отвечает за подробность лог-файла. При нормальной работе КриптоТуннеля не указывается.

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

6.1.1.1.2 Настройка параметров защищенных соединений

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

protocol может принимать значения http и rdp, кроме того, может быть не указана.

- `http` - указывает КриптоТуннелю, что защищаемый протокол - HTTP. В этом случае будут выполнены специфичные для этого протокола действия, например передача клиентского сертификата на веб-сервер.

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

- `rdp` - указывает, что защищаемый протокол - RDP. Также влияет на поведение серверной части.
- Опция protocol не указана. В этом случае сервером не будет предпринято никаких дополнительных действий. Следует использовать для протоколов, отличных от HTTP и RDP.

ciphers определяет набор шифров, использующихся для TLS-соединения. В большинстве случаев следует указывать GOST2012-GOST8912-GOST8912.

accept указывает, на каком адресе и порте (в формате address:port) КриптоТуннель будет ожидать внешнего подключения. Обычно это внешний адрес данного сервера и порт 443. Возможно указывать только порт (например, accept=443), в этом случае КриптоТуннель будет принимать соединения, пришедшие на указанный порт через любой сетевой интерфейс.

connect указывает, куда КриптоТуннель направит соединение, пришедшее на адрес, указанный в accept. Иными словами, это адрес бэк-энда, например веб- или RDP-сервера.

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

CRLfile указывает расположение файла со списком отзыва (или набором списков отзыва) сертификатов клиентов.

key указывает расположение файла закрытого ключа, используемого при установлении защищенного соединения.

cert указывает расположение файла сертификата открытого ключа, используемого при установлении защищенного соединения.

verify определяет, будет ли использована аутентификация клиента по сертификату, может принимать 3 значения:

0 означает, что сертификат клиента проверяться не будет, то есть к КриптоТуннелю сможет подключиться любой пользователь на совместимом ПО;

1 означает, что сертификат клиента будет проверяться, если клиент его предоставит. Промежуточный вариант между 0 и 2;

2 означает, что сертификат клиента будет требоваться и проверяться на соответствие сертификата УЦ, указанному в CAFile. Если сертификат истёк, выдан не доверенным УЦ, его нет и т.д., соединение будет отвергнуто сервером.

http_realip (только для протокола http) указывает, добавлять ли заголовок X-Real-IP с реальным адресом клиента, может принимать 3 значения:

no заголовок не добавляется;

yes (умолчание), заголовок добавляется только в случае его отсутствия;

force в случае отсутствия заголовка X-Real-IP он добавляется, при наличии замещается.

6.1.2 Ключевая инфраструктура

6.1.2.1 Серверная ключевая инфраструктура

Для того, чтобы после установки ПК «МагПро КриптоСервер» сервер 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, на котором подписан данный TLS-сертификат сервера.

Сертификат сервера, соответствующий ему закрытый ключ и корневой сертификат УЦ следует установить на сервере в соответствии с конфигурационным файлом «МагПро Крипто-

Пакет» в. 3.0 (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 серqвера 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>
2. Сертификат сервера должен содержать расширение Enhanced Key Usage со значением *Server Authentication (1.3.6.1.5.5.7.3.1)*.

6.1.2.2 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. Необходимо, чтобы сертификат клиента содержал расширение Enhanced Key Usage со значением *Client Authentication (1.3.6.1.5.5.7.3.2)*.

6.1.2.3 Формат файлов ключевой информации

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

6.2 Настройка клиента

6.2.1 Общие замечания

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» предназначен для того, чтобы можно было установить защищенное удаленное соединение или подписать документ, передаваемый через веб-форму, не выполняя никаких предварительных инсталляций. Поэтому настройка «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» сводится к указанию в конфигурационном файле удаленных объектов, с которыми следует устанавливать защищенное соединение, страниц, на которые следует перейти, и параметров электронной подписи.

В «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» имеются два файла, подлежащих редактированию: файл stunnel.conf и файл urls.

Основным конфигурационным файлом является файл stunnel.conf. Файл urls является дополнительным и служит для указания страниц, на которые следует переходить сразу же по установлении защищенного соединения с сайтом.

После того, как проведена описанная в данном разделе настройка «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» , настроенный «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» может быть скопирован на подключаемые носители (flash-устройства или лазерные диски) и предоставлен пользователям.

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

6.2.2 Настройка параметров защищенных соединений

6.2.2.1 Файл stunnel.conf

Файл stunnel.conf используется для указания адресов серверов, с которыми следует устанавливать TLS-соединение, и для указания адресов компьютеров, с которыми следует устанавливать RDP-соединение.

Процедура редактирования файла stunnel.conf:

1. Открыть файл stunnel.conf в текстовом редакторе;
2. Найти в файле stunnel.conf строку taskbar=yes. Все последующие дополнения вносятся после (ниже) этой строки;
3. Для конфигурирования TLS-соединения необходимо вписать следующую группу строк:
   (a) Строку, в которой содержится произвольная строка, состоящая из латинских букв и цифр и ограниченная квадратными скобками;
   (b) Строку вида accept=127.0.0.1:[номер локального порта];
   (c) Строку вида connect=[имя или IP-адрес https-сервера]:[номер порта https-сервера, к которому необходимо подключиться];
   (d) Строку ciphers=GOST2012-GOST8912-GOST8912;
   (e) Строку вида TIMEOUTclose=[значение].
4. Для конфигурирования RDP-соединения необходимо вписать следующую группу строк:
   (a) Строку, в которой содержится произвольная строка, состоящая из латинских букв и цифр и ограниченная квадратными скобками;
   (b) Строку protocol=rdp;
   (c) Строку вида alias=...
   (d) Строку вида accept=127.0.0.1:[номер локального порта];
   (e) Строку вида connect=[имя или IP-адрес удаленного компьютера]:[номер порта удаленного компьютера, к которому необходимо подключиться];
   (f) Строку ciphers=GOST2012-GOST8912-GOST8912;
   (g) Строку вида TIMEOUTclose=[значение].
5. Сохранить файл.

Каждая такая группа строк (секция) обозначает один сервер или удаленный компьютер, с которым можно установить защищенное-соединение (https- или rdp-соединение соответственно). Строка в квадратных скобках является наименованием секции. Параметр alias для rpd-соединения - это тот алиас, который будет выводиться в меню при запуске программы. В качестве значения параметра accept системным администратором назначается номер порта на 127.0.0.1, через который будет выполняться подключение к данному серверу или удаленному компьютеру. В качестве значения параметра connect указывается имя https-сервера или удаленного компьютера и номер его порта, через который выполняется подключение (следует узнать их у администратора сервера). Строка ciphers=GOST2012-GOST8912-GOST8912 указывает, какие алгоритмы шифрования следует использовать для защиты соединения. Параметр TIMEOUTclose указывает, сколько секунд следует ждать close_notify, рекомендуется во всех случаях устанавливать его значение в 0.

Если пользователю необходимо устанавливать защищенные соединения с несколькими серверами или удаленными компьютерами, для каждого сервера или удаленного компьютера необходимо вписать в файл stunnel.conf подобную группу строк. При этом следует учесть, что все указанные номера локальных портов, через которые устанавливаются защищенные соедине-

ния, должны быть разными, т.е. два соединения через один и тот же порт устанавливать нельзя.

Пример файла stunnel.conf для соединения с двумя серверами и с одним удаленным компьютером (для наглядности все секции отделены друг от друга пустыми строками):

```
verify=2
client=yes
CAFile=..\crypto\ca.crt
engine=cryptocom
engineCtrl=RNG:PROGRAM
engineCtrl=RNG_PARAMS:seed
error_image=error.png
output=stunnel.log
sslVersion=TLSv1
taskbar=yes

[someserver.ru]
accept = 127.0.0.1:8080
connect = tls.someserver.ru:443
ciphers = GOST2012-GOST8912-GOST8912
TIMEOUTclose = 0

[anotherserver.ru]
accept = 127.0.0.1:8083
connect = server.anotherserver.ru:443
ciphers = GOST2012-GOST8912-GOST8912
TIMEOUTclose = 1

[rdp-tls-s-w2--3-srv]
protocol=rdp
alias=Удаленный компьютер
accept=127.0.0.1:8085
connect=s-w2003-srv.servername.ru:13389
ciphers=GOST2012-GOST8912-GOST8912
TIMEOUTclose=0
```

В данном файле имеются две секции, описывающие параметры https-соединения с двумя серверами, и одна секция, описывающая параметры rdp-соединения с удаленным компьютером.

Первая секция описывает параметры https-соединения с сервером tls.someserver.ru. Для этого сервера назначен порт 8080 на 127.0.0.1, соединение выполняется через порт 443 на сервере.

Вторая секция описывает параметры https-соединения с сервером server.anotherserver.ru. Для этого сервера назначен порт 8083 на 127.0.0.1, соединение выполняется через порт 443 на сервере.

Третья секция описывает параметры rdp-соединения с удаленным компьютером s-w2003-srv.servername.ru. Для этого компьютера назначен порт 8085 на 127.0.0.1, соединение выполняется через порт 13389 на удаленном компьютере.

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

6.2.2.2 Файл urls

Файл urls используется для указания http-страниц, на которые следует перейти после установления защищенного соединения с серверами, а также для указания удобных алиасов для этих страниц.

Обратите внимание, что для RDP-соединения файл urls не нужен, алиасы rdp-соединений указываются прямо в файле stunnel.conf.

Для редактирования файла urls следует:

1. Открыть файл urls в текстовом редакторе;
2. Для каждого сервера вписать строку, в которой сначала указывается алиас сервера (должен быть уникален для каждого сервера), а затем через пробел указывается URL вида http://127.0.0.1:[номер локального порта]/<имя страницы на сервере>;
3. Сохранить файл.

Строки комментариев, если они есть, должны помечаться знаком #. Номер локального порта указывается тот, который был назначен в файле stunnel.conf для соединения с сервером, которому принадлежит указанный в данной строке алиас.

Алиас сервера может назначаться системным администратором произвольно. К алиасам имеются два требования:

1. Каждый алиас в файле urls должен быть уникальным (использоваться только один раз);
2. В алиасе не может быть пробелов.

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 нем 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.

Пример файла urls для соединения с двумя серверами, соответствующего вышеприведенному примеру для файла stunnel.conf:

```
#tls.someserver.ru
Интернет-магазин http://127.0.0.1:8080/params.cgi
#server.anotherserver.ru
Интернет-банк http://127.0.0.1:8083
```

Внимание. Если ссылка ведет не на страницу, а на каталог, необходимо указать в конце ссылки знак / (см. раздел **??**).

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 server.anotherserver.ru, т.к. для нее указан порт 8083 на 127.0.0.1, который в файле stunnel.conf указан как соответствующий серверу server.anotherserver.ru. Далее никаких страниц не указано, что означает, что при установлении tls-соединения пользователь увидит корневую страницу сервера server.anotherserver.ru.

6.2.3 Настройка клиентской аутентификации

Если сервер требует клиентской аутентификации, в конфигурационном файле stunnel.conf 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
```

Данные параметры указываются в головной секции конфигурационного файла, после параметра CAFile.

Значением параметра cert_sign является путь к пользовательскому (клиентскому) сертификату, значением параметра key_sign является путь к закрытому ключу пользователя.

6.2.4 Настройка параметров электронной подписи

Параметры электронной подписи указываются в файле конфигурации stunnel.conf.

Для того, чтобы задать тип подписи, в конфигурационном файле указывается параметр sign_type:

```
sign_type=[type_of_sign]
```

Значение параметра sign_type может быть ATTACHED или DETACHED. Если указано значение ATTACHED, будет вырабатываться подпись, передаваемая вместе с подписанным текстом. Если указано значение DETACHED, будет вырабатываться подпись, передаваемая отдельно от текста (а также метка времени).

По умолчанию на сайте ожидается, что передаваемые через web-форму документы подписываются подписью, передаваемой отдельно (тип DETACHED). Чтобы указать, что передаваемые документы подписываются подписью, которая передается вместе с документами (тип ATTACHED), необходимо, чтобы:

- web-форма содержала поле type_of_sign
- для этого поля было указано значение ATTACHED

Если оба эти условия не соблюдены, будет ожидаться подпись типа DETACHED.

6.2.4.1 Конфигурация подписи типа ATTACHED

Для того, чтобы «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» формировал электронную подпись типа ATTACHED, в конфигурационном файле stunnel.conf необходимо указать следующие опции:

```
cert_sign=[путь к файлу сертификатов пользователя в формате PEM]
key_sign=[путь к файлу закрытого ключа пользователя в формате PEM]
sign_inputs=[value_for_sign]
```

В качестве значения параметра sign_inputs, т.е. value_for_sign, может быть указан произвольный уникальный идентификатор.

Веб-форма на сайте должна содержать поле с внутренним наименованием, совпадающим со значением value_for_sign. Значение именно этого поля будет подписываться электронной подписью. Т.е. если через форму передаются файлы, то в данном поле следует реализовать выбор файла для подписи и передачи; если через форму передаются онлайн-запросы, то в данное поле следует вводить произвольный текстовый фрагмент запроса (например, стандартный текст запроса, сгенерированный на основе введенных пользователем данных). Конверт формата PKCS#7, содержащий подписанные данные и саму подпись, будет отправлен на сервер в этом же поле.

6.2.4.2 Конфигурация подписи типа DETACHED

Для того, чтобы «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» формировал электронную подпись типа DETACHED, в конфигурационном файле stunnel.conf необходимо указать следующие опции:

```
cert_sign=[путь к файлу сертификатов пользователя в формате PEM]
key_sign=[путь к файлу закрытого ключа пользователя в формате PEM]
sign_inputs=[value_for_sign]
sign_outputs=[value_for_detached_sign]
ts_input_url=[value_url_tsa]
ts_output=[value_time_stamp]
```

В качестве значений параметра sign_inputs, т.е. value_for_sign, параметра ts_input_url, т.е. value_url_tsa, и параметра ts_output, т.е. value_time_stamp, могут быть указаны произвольные уникальные идентификаторы.

Веб-форма на сайте должна содержать:

- поле с внутренним наименованием, совпадающим со значением value_for_sign. Значение именно этого поля будет подписываться электронной подписью.
- поле с внутренним наименованием, совпадающим со значением value_url_tsa. В этом поле должен быть задан URL службы TSA, в которой следует получить временную метку.
- поле с внутренним наименованием, совпадающим со значением value_time_stamp. При создании подписи типа DETACHED «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» формирует запрос для службы TSA, отправляет запрос на указанный URL, получает ответ на этот запрос и помещает его в качестве значения поля value_time_stamp в формате base64.

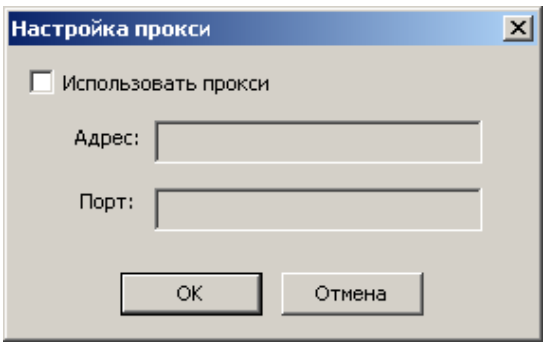
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Следует иметь в виду, что при подписи и загрузке на сервер файла со наименованием `[имя файла]` подпись типа DETACHED будет загружаться на сервер в виде файла с наименованием `[имя файла].p7`, а временная метка — в виде файла с наименованием `[имя файла].p7.ts`.

6.2.5 Настройка «КриптоТуннель» для работы через прокси-сервер

Пользователь может самостоятельно настроить «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» для работы через прокси-сервер. Для этого при первом запуске необходимо:

1. Щелкнуть правой клавишей мыши по иконке «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» в трее;
2. В появившемся контекстном меню выбрать «Прокси». Появится окно настройки прокси:



3. Поставить галочку «Использовать прокси»;
4. Указать адрес и порт прокси-сервера. Необходимые адрес и порт можно узнать из настроек Internet Explorer: Пункт меню «Сервис» — подпункт «Свойства обозревателя» — страница «Подключения» — кнопка «Настройка LAN». В появившемся окне «Настройка локальной сети» в группе параметров «Прокси-сервер» указаны адрес и порт прокси-сервера. Скопировать их в соответствующие поля в окно настройки прокси «КриптоТуннель» .
   Можно также уточнить адрес и порт прокси-сервера у администратора локальной сети.
5. Нажать кнопку Ок.

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

7 Использование

7.1 Использование серверной части для ОС семейства Windows

После выполнения процедуры настройки «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» готов к работе.

7.2 Использование клиентской части для ОС семейства Windows

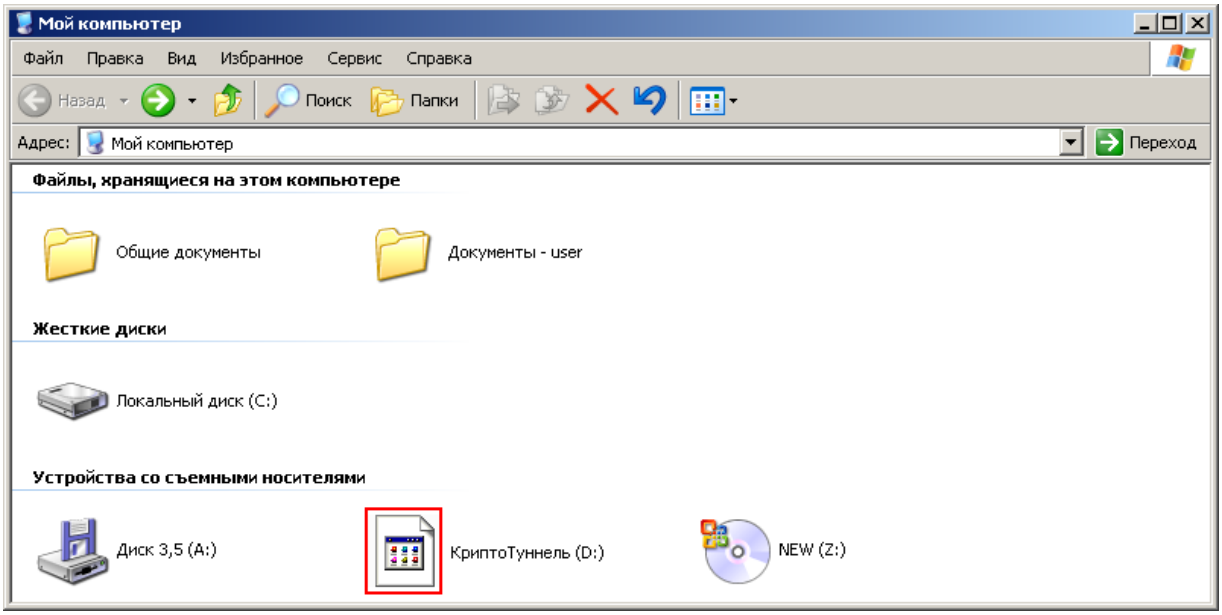
7.2.1 Запуск «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель»

Для того, чтобы начать работу с «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» , следует подключить носитель (flash-устройство или лазерный диск) с установленным программным комплексом к компьютеру.

Если на компьютере включен autorun, то при подключении носителя программный комплекс запускается автоматически.

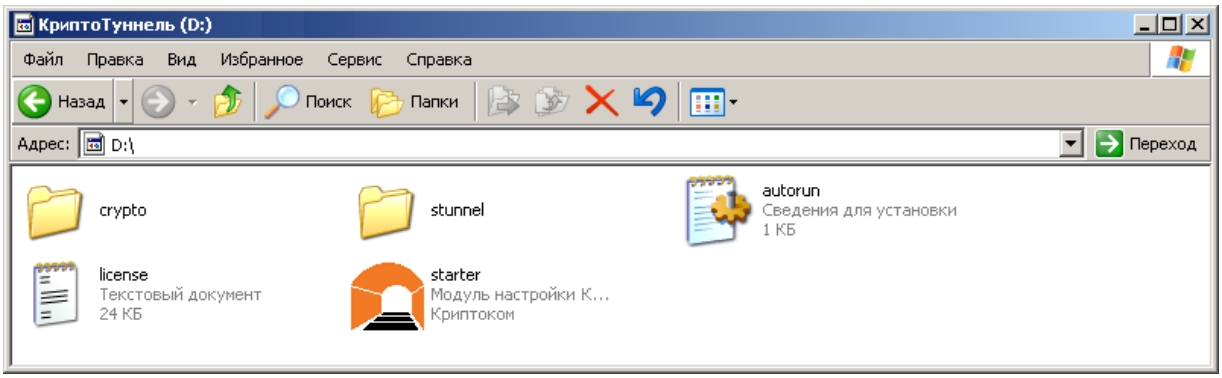
Если autorun не включен, необходимо запустить «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» через окно «Мой компьютер». Для этого необходимо:

1. Дважды щелкнув мышью на иконке «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» (на рисунке отмечена красной рамкой), открыть содержание носителя с «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» :

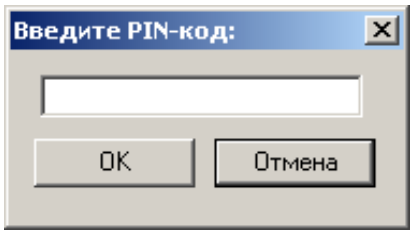


Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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

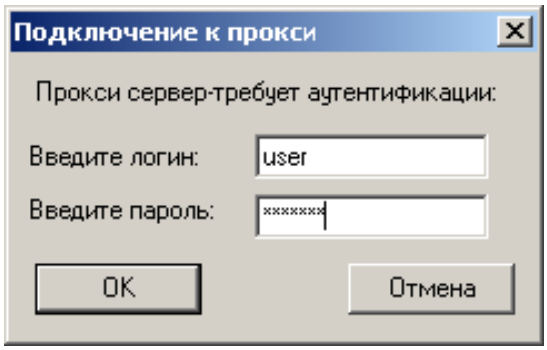


Если закрытый ключ пользователя защищен PIN-кодом, то после запуска «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» выводится окно запроса PIN-кода ключа:



Необходимо указать в поле ввода PIN-код ключа и нажать кнопку OK.

Если пользователь использует прокси-сервер, требующий аутентификации, то при запуске «КриптоТуннель» (после ввода PIN-кода, если таковой производится) потребуется явная аутентификация на прокси-сервере:



Пользователю необходимо явным образом ввести логин и пароль для аутентификации на прокси-сервере, даже если при обычной работе эта аутентификация выполнялась браузером автоматически.

Логин и пароль необходимо узнать у администратора прокси-сервера.

«КриптоТуннель» поддерживает два способа аутентификации через прокси-сервер: basic (с использованием логина и пароля, заданных на прокси-сервере) и NTLM (с использованием доменного логина и пароля). Какой именно способ аутентификации применяется, зависит от настроек прокси-сервера. Если прокси-сервер настроен так, что при аутентификации он предлагает выбор способа аутентификации, то «КриптоТуннель» всегда выбирает NTLM, т.е. необходимо вводить доменный логин и пароль.

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

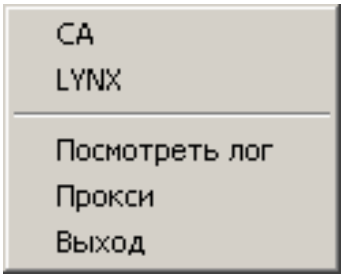
Т.е. если прокси-сервер требует аутентификации basic, необходимо вводить логин и пароль, заданные на прокси-сервере; если прокси-сервер требует способ аутентификации NTLM или предлагает выбор способа аутентификации, необходимо вводить доменный логин и пароль. Это следует знать, обращаясь к администратору прокси-сервера.

7.2.2 Контекстное меню

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

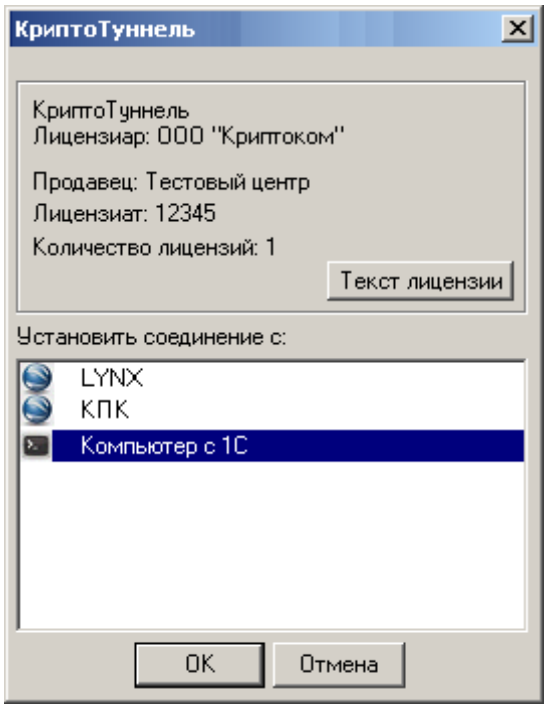
Контекстное меню состоит из двух частей. В верхней части выводится список серверов, с которыми можно установить защищенное соединение. В нижней части выводятся служебные пункты: «Посмотреть лог» (см. раздел 7.2.8), «Прокси» (см. раздел 6.2.5) и «Выход» (см. раздел 7.2.6).

Пример контекстного меню:



7.2.3 Установление защищенных соединений

Если в конфигурационном файле stunnel.conf указано более одного объекта для установления защищенного соединения (серверы или удаленные компьютеры), или указан только удаленный компьютер для установления соединения по RDP, то выводится окно, в верхней части которого находится отображение лицензии, а в нижней — меню, предоставляющее выбор объекта, с которым следует установить соединение:



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

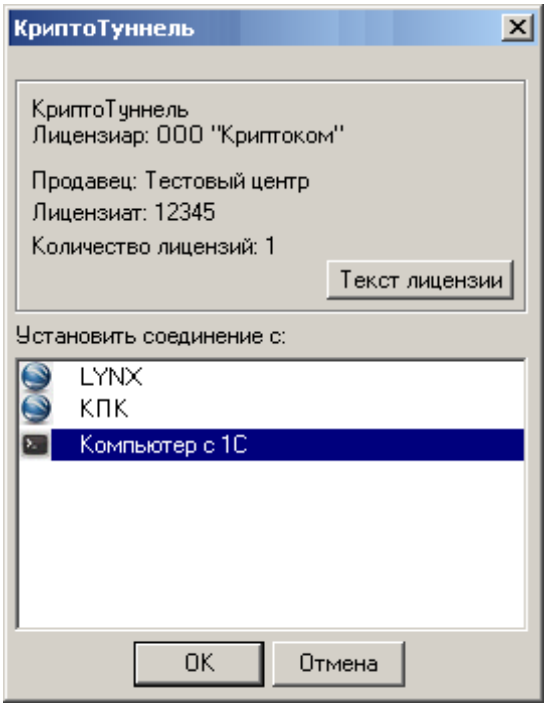
В данном меню указаны алиасы двух серверов, с которыми нужно устанавливать https-соединение — LYNX и КПК, а также алиас удаленного компьютера, с которым нужно устанавливать rdp-соединение - Компьютер с 1С.

Следует щелкнуть мышью по названию необходимого объекта и нажать на кнопку «Ок». Будет установлено защищенное соединение с выбранным объектом. Если выбрано https-соединение, то запускается браузер, в котором открывается необходимая пользователю страница; если выбрано rdp-соединение, то открывается окно, содержащее рабочий стол удаленного компьютера. В трее (в правой нижней части экрана) появляется иконка «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» :

Если нажать кнопку «Отмена», никакого соединения не устанавливается, но «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» продолжает работу, иконка в трее остается.

Установить соединение с сайтом в этом случае можно двумя способами:

– Либо дважды щелкнуть левой клавишей мыши по иконке «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» в трее. В этом случае выводится окно, в верхней части которого находится отображение лицензии, а в нижней — меню, предоставляющее выбор объекта, с которым следует установить соединение:



Подобное окно выводится при двойном щелчке левой клавишей мыши по иконке «МагПро КриптоПакет» в. 3.0 в трее и в том случае, если в конфигурационном файле указан только один объект.

Следует щелкнуть мышью по алиасу необходимого объекта (если объект только один — по его алиасу) и нажать на кнопку «Ок». Будет установлено защищенное соединение с выбранным объектом.

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

– Либо щелкнуть правой кнопкой мыши по иконке «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» в трее. Появится контекстное меню, содержащее:
  1. названия объектов, указанных в конфигурационном файле;
  2. пункт «Просмотреть лог»;
  3. пункт «Выход».

  Следует щелкнуть мышью по алиасу необходимого объекта (если объект только один — по его алиасу). Будет установлено защищенное соединение с указанным объектом.

После установления защищенного соединения открывается соответствующее окно.

Если при установленном соединении навести курсор на иконку «КриптоТуннель» в трее, всплывает комментарий, содержащий техническую информацию о защищенном соединении: название работающей программы, имя удаленного объекта с портом подключения и алгоритмы, использованные для защиты соединения (если это алгоритмы ГОСТ, то выводится просто GOST).

Пример такого всплывающего комментария:

```
МагПро КриптоПакет 3.0, исполнение КриптоТуннель
ca.cryptocom.ru:443 GOST
```

Если в конфигурационном файле указан только один объект для установления удаленного соединения, то при запуске «КриптоТуннель» автоматически устанавливается защищенное соединение с этим объектом. Запускается браузер, в котором открывается необходимая пользователю страница, или открывается окно рабочего стола удаленного компьютера. Выводится также всплывающее пояснение: *Для перехода по ссылкам, щелкните правой кнопкой мыши по иконке*.

7.2.4 При длительной работе «КриптоТуннель»

Если «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» запущен какое-то время назад, и меню выбора удаленного объекта на экране нет, необходимо:

1. Дважды щелкнуть левой клавишей мыши по иконке «КриптоТуннель» в трее. Будет выведено меню выбора удаленного объекта
2. Щелкнуть мышью по алиасу необходимого объекта
3. Нажать на кнопку «Ок».

Либо:

1. Щелкнуть правой кнопкой мыши по иконке «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» в трее. Появится контекстное меню, содержащее названия удаленных объектов
2. Щелкнуть мышью по алиасу необходимого объекта
3. Нажать на кнопку «Ок».

7.2.5 Выработка электронной подписи под онлайн-запросом или файлом, передаваемым через веб-форму

Если в конфигурационном файле «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» указаны параметры электронной подписи, то после установления защищенного соединения с сайтом, на котором находится веб-форма для передачи на сервер подписанных данных, можно с помощью «КриптоТуннель» подписывать электронной подписью и отправлять на сервер онлайн-запросы или файлы.

Конкретная процедура отправки онлайн-запроса или файла определяется администратором сайта. Подписывание данных может быть автоматическим или после подтверждения пользователем.

Чтобы отправить на сервер подписанный файл или онлайн-запрос, следует после установления защищенного соединения с сайтом, содержащим веб-форму, выполнять инструкции, приведенные на сайте.

1. Запустить «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель»
2. С помощью «КриптоТуннель» установить защищенное соединение с сайтом, на котором находится веб-форма
3. Заполнить веб-форму в соответствии с инструкциями, приведенными на сайте, и отправить данные на сервер
4. Если веб-форма запрашивает подтверждение подписи под отправляемыми данными, проверить их и подтвердить подпись.

7.2.6 Выход из программы

Для выхода из программы необходимо:

1. Щелкнуть правой клавишей мыши по иконке «КриптоТуннель» в трее (в правой нижней части экрана);
2. В появившемся контекстном меню щелкнуть левой кнопкой мыши по пункту «Выход».

7.2.7 Лицензирование программного комплекса

«МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» предоставляется пользователю на съемном носителе (flash-устройство или лазерный диск) в полностью готовом к работе состоянии.

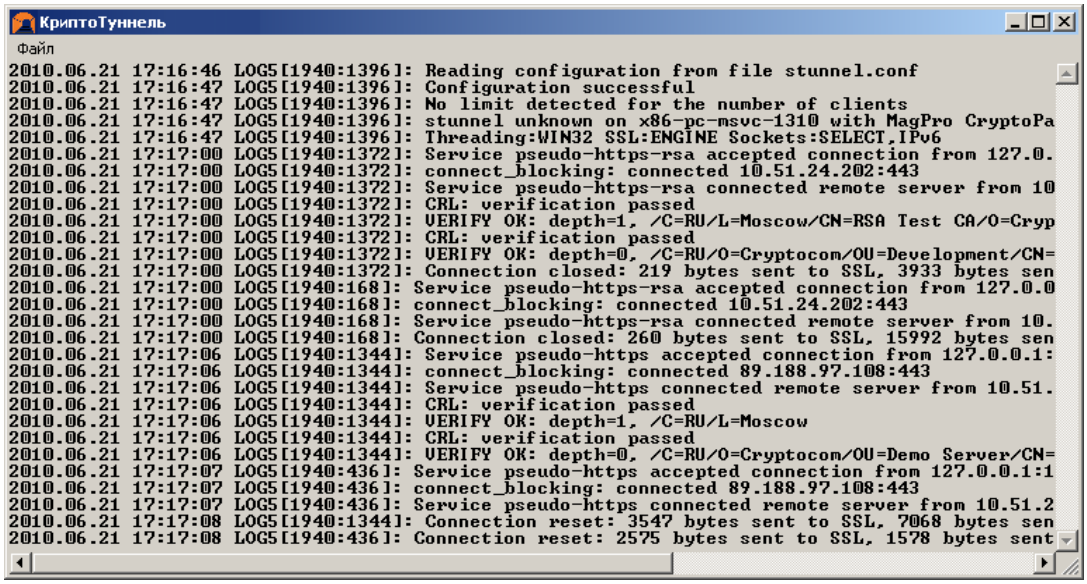
Вместе с каждым экземпляром «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» пользователю предоставляется лицензия на данный продукт. Лицензия может иметь ограниченный срок действия. В этом случае за 2 месяца до окончания срока действия при запуске «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» начинает предупреждать о приближающемся окончании срока действия. Пользователю следует обратиться к Вашему поставщику «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» за новой лицензией.

7.2.8 Журнал работы «КриптоТуннель»

Журнал работы «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» содержит информацию о всех операциях, выполненных «КриптоТуннель» с момента последнего запуска. Эта информация может быть полезна для системного администратора при возникновении каких-либо ошибок при работе «КриптоТуннель» (см. раздел 8).

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 «Посмотреть лог». 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.

7.3 Использование серверной части для 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 запусть программу

```
sudo /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, «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» готов к работе. Запуск сервера осуществляется командой

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

7.4 Использование клиентской части для 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 запусть программу

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

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

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, «МагПро КриптоПакет» в. 3.0 в исполнении «КриптоТуннель» готов к работе. Запуск осуществляется командой

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

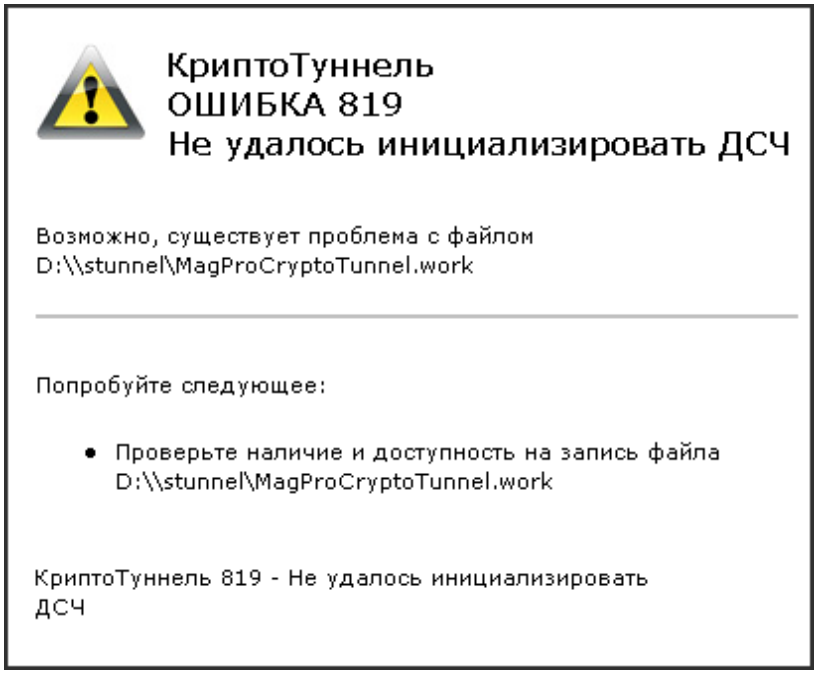
Для установления соединения с web-сервером, защищённым по протоколу TLS с использованием алгоритмов ГОСТ, нужно в ввести в браузере адрес:порт, указанные в файле конфигурации в параметре accept.

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

8 Сообщения оператору

8.1 Общие замечания

Если при работе «МагПро КриптоПакет» в. 3.0 возникает ошибка, появляется экран с сообщением:



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. Если Вы не знаете, как связаться с администратором сервера, обратитесь к Вашему поставщику «МагПро КриптоПакет» в. 3.0.

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

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 отредактированы конфигурационные файлы stunnel.conf и urls (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 тому лицу, которое создает сертификаты для сервера (администратор УЦ или администратор сервера), и попросить создать сертификат сервера, срок действия которого наступает сразу же. Попросить администратора сервера установить этот сертификат на сервере.
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 тому лицу, которое создает сертификаты для сервера (администратор УЦ или администратор сервера), и попросить создать новый сертификат сервера. Попросить администратора сервера установить этот сертификат на сервере.
815	Сервер неожиданно прервал соединение	Возможно, в работе сервера произошел сбой	Попробуйте установить соединение позднее

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

Код ошибки	Ошибка	Причина	Действия оператора
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.
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 отредактированы конфигурационные файлы stunnel.conf и urls (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	Выясните у администратора сервера, включена ли у него поддержка TLS. При необходимости попросите его включить поддержку TLS, если это возможно. Если проблема не исчезает, обратитесь в службу поддержки ООО «Криптоком».
819	Не удалось инициализировать ДСЧ	Возможно, существует проблема с файлом <полный путь к файлу MagProCryptoTunnel.work>	Проверьте наличие и доступность на запись файла <полный путь к файлу MagProCryptoTunnel.work>
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.

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

Код ошибки	Ошибка	Причина	Действия оператора
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 6.2.3.
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 Ошибки при работе через прокси-сервер

Код ошибки	Ошибка	Причина	Действия оператора
407	Вам не удалось аутентифицироваться на прокси-сервере	Возможно, Вы допустили ошибку при вводе логина или пароля	Установите соединение заново
408	Вам не удалось аутентифицироваться на прокси-сервере	КриптоТуннель не поддерживает схему аутентификации, предложенную прокси-сервером	Обратитесь к администратору локальной сети
409	Вам не удалось аутентифицироваться на прокси-сервере	Прокси-сервер не предложил схему аутентификации	Обратитесь к администратору локальной сети
410	Не удалось установить соединение через прокси-сервер	Возможно, прокси-сервер не смог подключиться к сайту	Обратитесь к администратору локальной сети

8.4 Ошибки при работе с лицензиями и каталогами

Ошибка	**Причина**	**Действия оператора**
Не удалось получить текущую директорию. Работа программы будет прервана. Возникновение данной проблемы свидетельствует о наличии серьёзных сбоев в работе Windows. Обратитесь к Вашему системному администратору.	Сбой в работе системы	Обратитесь к администратору, обслуживающему Ваш компьютер
Не удалось открыть файл лицензии	Файл лицензии не существует или поврежден	Обратитесь к лицу, выдавшему Вам «МагПро КриптоПакет» в. 3.0, и попросите оформить для вас новый файл лицензии в соответствии с условиями лицензирования
При старте программы произошла ошибка. Вам следует передать служебную информацию системному администратору. Для получения служебной информации нажмите OK.	Программный сбой	Нажмите OK и вызовите администратора, обслуживающего Ваш компьютер
Не найден файл лицензии. Работа программы невозможна.	Файл лицензии не существует или поврежден	Обратитесь к лицу, от которого Вы получили «МагПро КриптоПакет» в. 3.0, и попросите оформить для вас новый файл лицензии в соответствии с условиями лицензирования
Срок действия Вашей лицензии истек. Работа программы невозможна.	Срок действия лицензии истек	Обратитесь к лицу, от которого Вы получили «МагПро КриптоПакет» в. 3.0, и попросите оформить для вас новый файл лицензии в соответствии с условиями лицензирования

Ошибка	Причина	Действия оператора
Файл лицензии поврежден (код ошибки <код ошибки>). Работа программы невозможна.	Файл лицензии не существует или поврежден	Обратитесь к лицу, от которого Вы получили «МагПро КриптоПакет» в. 3.0, и попросите оформить для вас новый файл лицензии в соответствии с условиями лицензирования

8.5 Предупреждение о скором окончании срока действия лицензии

ВНИМАНИЕ!!! Ваша лицензия истекает <дата истечения лицензии>

Следует обратиться к лицу, от которого Вы получили «МагПро КриптоПакет» в. 3.0, для оформления новой лицензии в соответствии с условиями лицензирования.

8.6 Всплывающие сообщения

Сообщения, всплывающие над иконкой «МагПро КриптоПакет» в. 3.0 в трее

Ошибка	Причина	Действия оператора
Страница, на которую Вы попытались пойти, неправильно описана в конфигурационном файле URLS. Обратитесь к администратору.	Неправильно настроены конфигурационные файлы «МагПро КриптоПакет» в. 3.0	Обратитесь к лицу, от которого вы получили «МагПро КриптоПакет» в. 3.0
Не удалось запустить обозреватель интернета. Попробуйте запустить обозреватель интернета вручную и зайти на страницу <адрес страницы из файла URLS, на которую пытался зайти юзер>	Скорее всего, браузер по умолчанию некорректно зарегистрирован в системе	Запустите браузер вручную и введите адрес, указанный в сообщении, тем самым обходя некорректную регистрацию браузера в системе.

9 Приложения

9.1 Файлы сертификатов

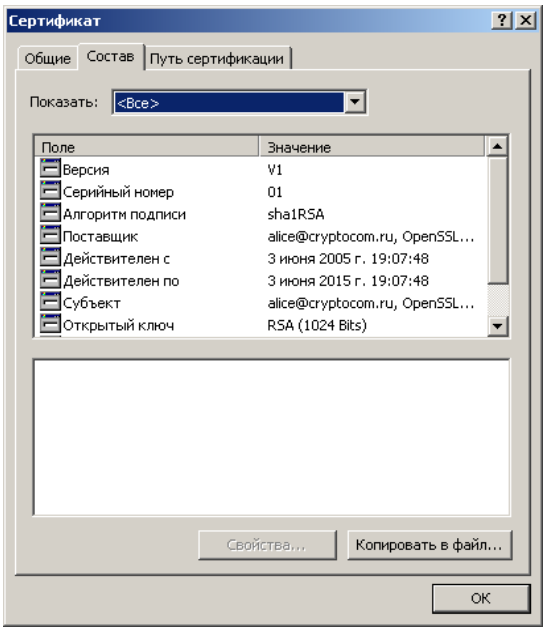
9.1.1 Файл сертификатов УЦ

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).

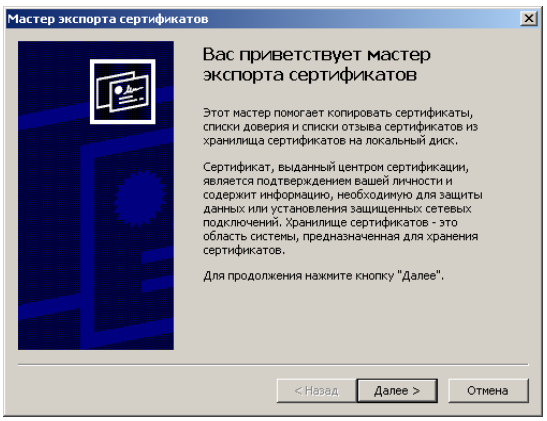
Сертификаты в этом файле должны быть в формате PEM. Если сертификат УЦ получен в формате DER (расширения .cer или .crt) или PKCS#7 (расширение p7b), то можно воспользоваться системными средствами Windows для конвертации его в формат PEM.

Конвертирование файлов формата DER (расширения .cer или .crt) в формат PEM:

1. Двойным щелчком мыши открыть сертификат для просмотра и перейти на страницу «Состав»:



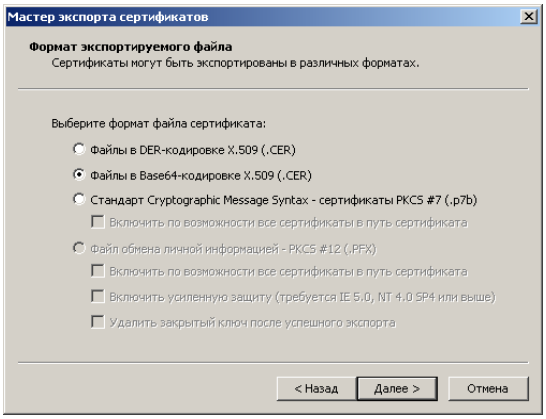
2. Нажать на кнопку «Копировать в файл». Запустится мастер экспорта сертификатов;



Нажать на кнопку «Далее».

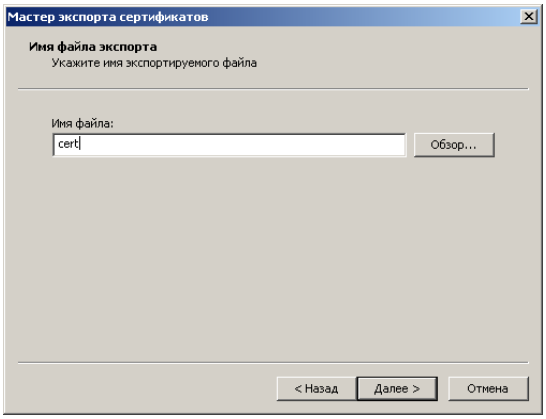
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Откроется окно выбора формата файлов. Выбрать второй пункт в списке форматов (Файлы в Base-64 кодировке X.509):

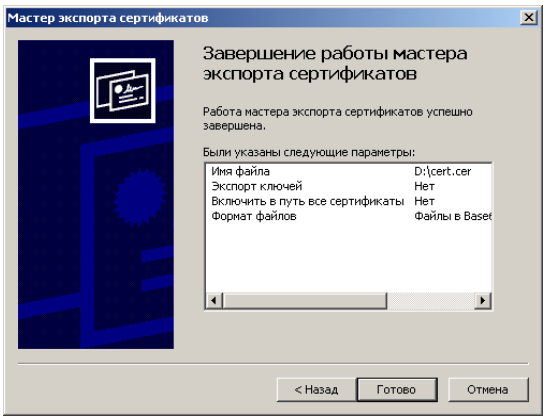


и нажать на кнопку «Далее»;

4. Указать имя файла, в который копируется сертификат в выбранном формате, и нажать на кнопку «Далее»;



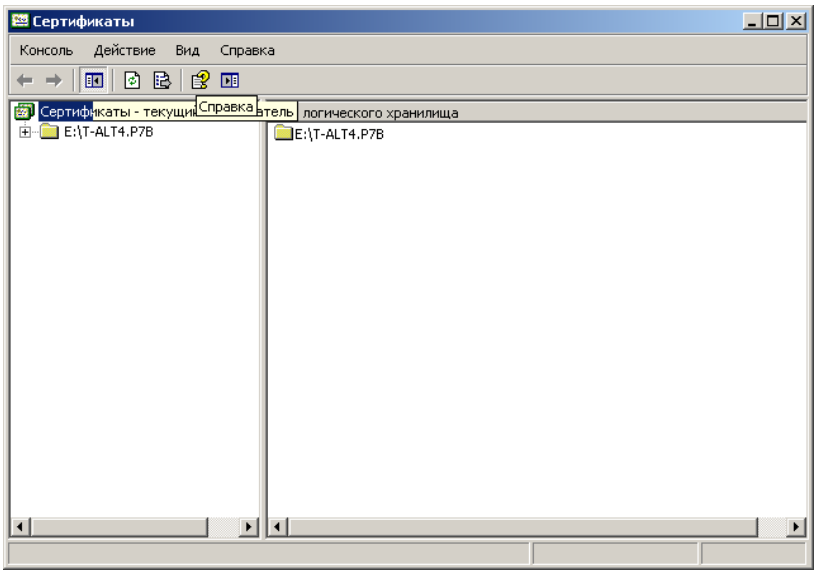
5. Нажать на кнопку «Готово».



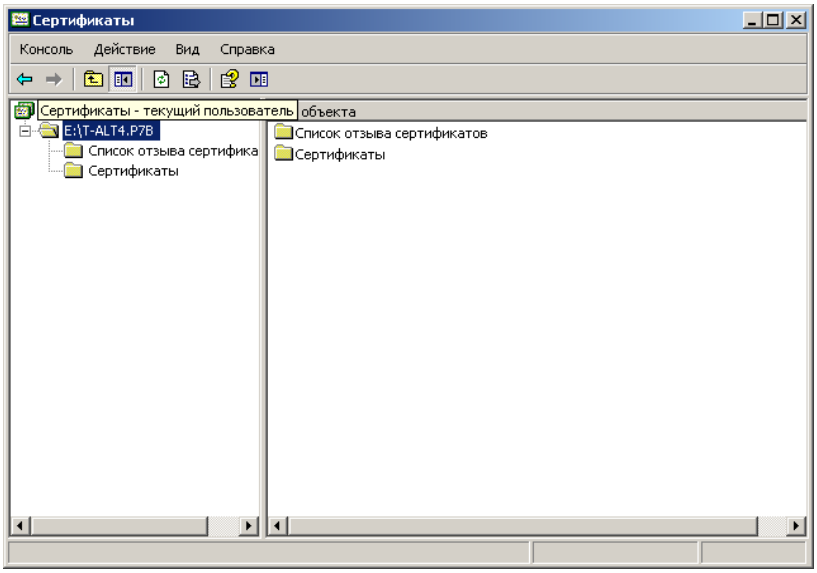
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Конвертирование файла формата PKCS#7 (расширение p7b) в формат PEM:

1. Двойным щелчком мыши открыть окно просмотра цепочки сертификатов:

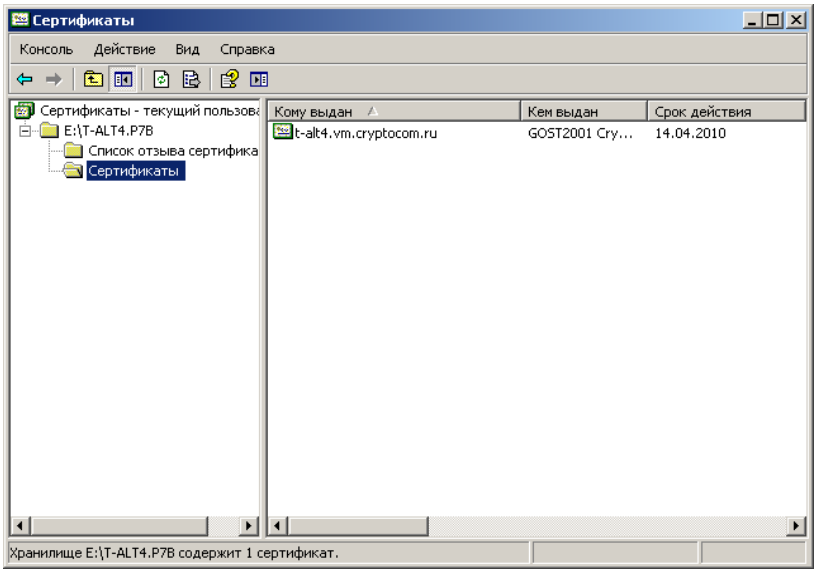


2. Щелчком мыши по наименованию цепочки сертификатов раскрыть ее содержание:



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

3. Щелчком мыши на пункте «Сертификаты» вывести в правой части окна название сертификата:



4. Двойным щелчком мыши на названии сертификата в правой части окна открыть окно просмотра сертификата. Дальнейшая работа выполняется так же, как при конвертации сертификатов в формате DER, описанной выше.

Полученный файл сертификата в Base-64 кодировке X.509 и есть файл в формате PEM. Его следует открыть в текстовом редакторе, где он будет выглядеть следующим образом:

```
-----BEGIN CERTIFICATE-----
[Содержимое сертификата]
-----END CERTIFICATE-----
```

Сертификат в формате PEM следует вместе с заголовочными строками (строки с дефисами) скопировать в файл сертификатов, который использует «МагПро КриптоПакет» в. 3.0.

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, необходимо создать для каждого пользователя файл сертификатов, содержащий открытый ключ, и файл закрытого ключа, и зарегистрировать сертификат пользователя. В конфигурационный файл stunnel.conf необходимо добавить параметры клиентской аутентификации, как описано в разделе 6.2.3.

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

9.2 Адреса страниц, приводящие к разрыву https-соединения

Когда пользователь, установив защищенное соединение с сервером с помощью «МагПро КриптоПакет» в. 3.0, 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.

9.2.1 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.

9.2.2 Адреса каталогов

Если с использованием клиентской части «МагПро КриптоПакет» в. 3.0 устанавливается соединение с web-сервером, в который встроена поддержка алгоритмов ГОСТ, то все ссылки на каталоги должны заканчиваться на /, иначе корректный переход по этой ссылке будет невозможен (при отсутствии завершающего слеша сервер выполняет редирект на адрес со знаком / по протоколу HTTPS, в результате чего также происходит попытка установить новое HTTPS-соединение напрямую, а так как сам браузер не может работать с алгоритмами ГОСТ, такое соединение установить не удаётся).

Если поддержка алгоритмов ГОСТ на сервере обеспечивается средствами серверной части «МагПро КриптоПакет» в. 3.0, такой проблемы не возникает, все ссылки на каталоги обрабатываются корректно.

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