КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00017-01 34 01 - ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС
МагПро КриптоТуннель вер. 1.0

Руководство оператора

СЕИУ.00017-01 34 01
Листов 39

Литера О

2011

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

Аннотация

Настоящий документ содержит руководство оператора для работы с ПК «МагПро КриптоТуннель».

Авторские права на ПК «МагПро КриптоТуннель» принадлежат ООО «Криптоком».

В коде ПК использован код OpenSSL, ©1998-2004, The OpenSSL Project.

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

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

ПК «МагПро КриптоТуннель» позволяет:

1. установить соединение с сервером, защищенное по протоколу TLS (HTTPS-соединение), с использованием алгоритмов GOST, не меняя содержания файлов, содержащихся на компьютере пользователя;
2. установить защищенное RDP-соединение с удаленным компьютером;
3. выработать электронную цифровую подпись под текстовыми данными или файлом, которые передаются пользователем через веб-форму;
4. выработать метку времени для подписи, заверенную в службе временных меток.

Электронная цифровая подпись может передаваться как вместе с подписанным документом, так и отдельно от него. При отдельной передачи подписи ПК «МагПро КриптоТуннель» создает метку времени для подписи, заверенную в службе временных меток.

2 УСЛОВИЯ РАБОТЫ ПРОГРАММНОГО КОМПЛЕКСА

ПК «МагПро КриптоТуннель» предназначен для работы в ОС Windows 2000/2000 Server/XP/2003 Server/Vista/Windows 7/2008 Server.

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

3 СОСТАВ ПРОГРАММНОГО КОМПЛЕКСА

В состав программного комплекса входят:

1. Программа stunnel
2. СКЗИ МагПро КриптоПакет
3. Программа автоматического запуска
4. Программа starter для вызова СКЗИ МагПро КриптоПакет из stunnel
5. Файл сертификатов удостоверяющих центров в формате PEM
6. Конфигурационные файлы

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

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

4 ЛИЦЕНЗИРОВАНИЕ ПРОГРАММНОГО КОМПЛЕКСА

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

Вместе с каждым экземпляром ПК «МагПро КриптоТуннель» пользователю предоставляется лицензия на данный продукт. Без действующей лицензии ПК «МагПро КриптоТуннель» не запускается.

Лицензия может иметь ограниченный срок действия. В этом случае за 2 месяца до окончания срока действия при запуске ПК «МагПро КриптоТуннель» начинает предупреждать о приближающемся окончании срока действия. Пользователю следует обратиться к Вашему поставщику ПК «МагПро КриптоТуннель» за новой лицензией.

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

5 КРАТКОЕ ОПИСАНИЕ ВЫПОЛНЕНИЯ ОСНОВНЫХ ОПЕРАЦИЙ

5.1 Запуск ПК «МагПро КриптоТуннель»

Если на компьютере включен autorun:

1. Подключить носитель (flash-устройство или лазерный диск) к компьютеру
2. Программный комплекс запускается автоматически.

Если на компьютере отключен autorun:

1. Дважды щелкнув мышью на иконке носителя, содержащего ПК «МагПро КриптоТуннель», открыть содержание носителя
2. Дважды щелкнуть мышью по иконке starter

Подробное описание выполнения операций см. в разделе 7.1.

5.2 Ввод PIN-кода

Если после запуска ПК «МагПро КриптоТуннель» запрашивает PIN-код, необходимо:

1. Указать в поле ввода PIN-код ключа
2. Нажать кнопку ОК.

Подробное описание выполнения операций см. в разделе 7.2.

5.3 Аутентификация на прокси-сервере

Если пользователь работает через требующий аутентификации прокси-сервер, после запуска ПК «МагПро КриптоТуннель» (ввода PIN-кода, если требуется) выводится окно аутентификации на прокси-сервере. Необходимо:

1. ввести логин и пароль для аутентификации на прокси-сервере
2. Нажать кнопку ОК.

Подробное описание выполнения операций см. в разделе 7.3.

5.4 Установление защищенного соединения

Подробное описание выполнения операций см. в разделе 8.1.

5.4.1 При запуске ПК «МагПро КриптоТуннель»

Если ПК «МагПро КриптоТуннель» предназначен для установления защищенного соединения с одним удаленным объектом, то защищенное соединение устанавливается автоматически.

Если удаленных объектов (сайтов или удаленных компьютеров), с которыми данный экземпляр ПК «МагПро КриптоТуннель» может устанавливать защищенное соединение, более одного, то при запуске ПК «МагПро КриптоТуннель» выводится меню, предоставляющее выбор объекта. Необходимо:

1. Щелкнуть мышью по алиасу необходимого объекта
2. Нажать на кнопку «Ок»

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

5.4.2 При длительной работе ПК «МагПро КриптоТуннель»

Если ПК «МагПро КриптоТуннель» запущен какое-то время назад, и меню выбора удаленного объекта на экране нет, необходимо:

1. Дважды щелкнуть левой клавишей мыши по иконке ПК «МагПро 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 ПК «МагПро КриптоТуннель» в трее. Появится контекстное меню, содержащее названия удаленных объектов
2. Щелкнуть мышью по алиасу необходимого объекта
3. Нажать на кнопку «Ок».

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

1. Запустить ПК «МагПро КриптоТуннель»
2. С помощью ПК «МагПро 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.

Подробное описание выполнения операций см. в разделе 8.2.

5.6 Выход из программы

Чтобы выйти из ПК «МагПро КриптоТуннель», необходимо:

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

6 НАСТРОЙКА ПРОГРАММНОГО КОМПЛЕКСА

6.1 Общие замечания

ПК «МагПро 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 ПК «МагПро КриптоТуннель» сводится к указанию в конфигурационном файле удаленных объектов, с которыми следует устанавливать защищенное соединение, страниц, на которые следует перейти, и параметров электронной цифровой подписи.

В ПК «МагПро 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 ПК «МагПро КриптоТуннель», настроенный ПК «МагПро КриптоТуннель» может быть скопирован на подключаемые носители (flash-устройства или лазерные диски) и предоставлен пользователям.

Следует иметь в виду, что в состав ПК «МагПро КриптоТуннель» входит файл инициализации ДСЧ MagProCryptoTunnel.work, содержание которого меняется при запуске ПК «МагПро КриптоТуннель». Поэтому, если ПК «МагПро КриптоТуннель» записан на защищенном от записи носителе (лазерном диске), файл MagProCryptoTunnel.work копируется в место, указанное переменной окружения %TEMP%, и ПК «МагПро КриптоТуннель» пользуется для работы именно этой копией файла MagProCryptoTunnel.work.

6.2 Настройка параметров защищенных соединений

6.2.1 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=GOST2001-GOST89-GOST89;
   (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;

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

(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=GOST2001-GOST89-GOST89;
(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=GOST2001-GOST89-GOST89 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 соединения, 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 = GOST2001-GOST89-GOST89
TIMEOUTclose = 0

[anotherserver.ru]
```

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

```
accept = 127.0.0.1:8083
connect = server.anotherserver.ru:443
ciphers = GOST2001-GOST89-GOST89
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=GOST2001-GOST89-GOST89
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.

6.2.2 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 ПК «МагПро КриптоТуннель» в контекстом меню, которое пользователь вызывает щелчком правой кнопки мыши по иконке ПК «МагПро КриптоТуннель» в трее, выводится именно список алиасов серверов. Этот же список выводится в качестве меню при запуске ПК «МагПро 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 11.2.2).

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 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.

6.3 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.

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

6.4 Настройка параметров электронной цифровой подписи

Параметры электронной цифровой 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.

6.4.1 Конфигурация подписи типа ATTACHED

Для того, чтобы ПК «МагПро КриптоТуннель» формировал электронную цифровую 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 цифровой 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.

6.4.2 Конфигурация подписи типа DETACHED

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

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

```
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:

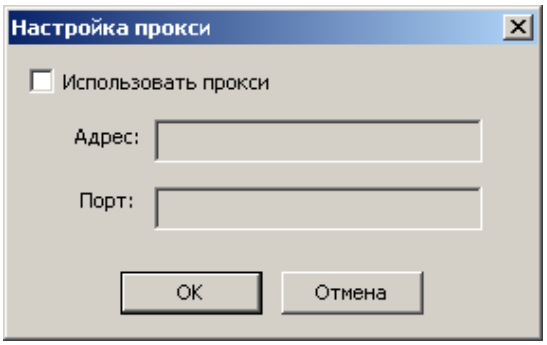
- поле с внутренним наименованием, совпадающим со значением value_for_sign. Значение именно этого поля будет подписываться электронной цифровой подписью.
- поле с внутренним наименованием, совпадающим со значением value_url_tsa. В этом поле должен быть задан URL службы TSA, в которой следует получить временную метку.
- поле с внутренним наименованием, совпадающим со значением value_time_stamp. При создании подписи типа DETACHED ПК «МагПро 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.

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`.

6.5 Настройка ПК МагПро КриптоТуннель для работы через прокси-сервер

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

1. Щелкнуть правой клавишей мыши по иконке ПК «МагПро 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 ПК «МагПро 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 ЗАПУСК ПРОГРАММЫ

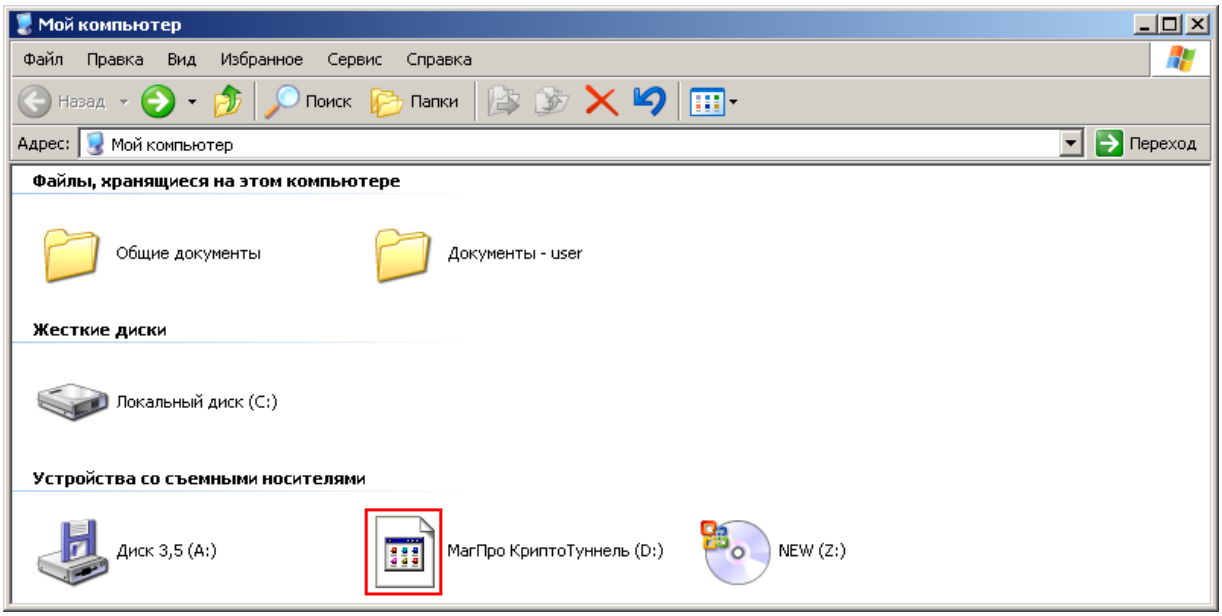
7.1 Запуск программы

Для того, чтобы начать работу с ПК «МагПро КриптоТуннель», следует подключить носитель (flash-устройство или лазерный диск) к компьютеру.

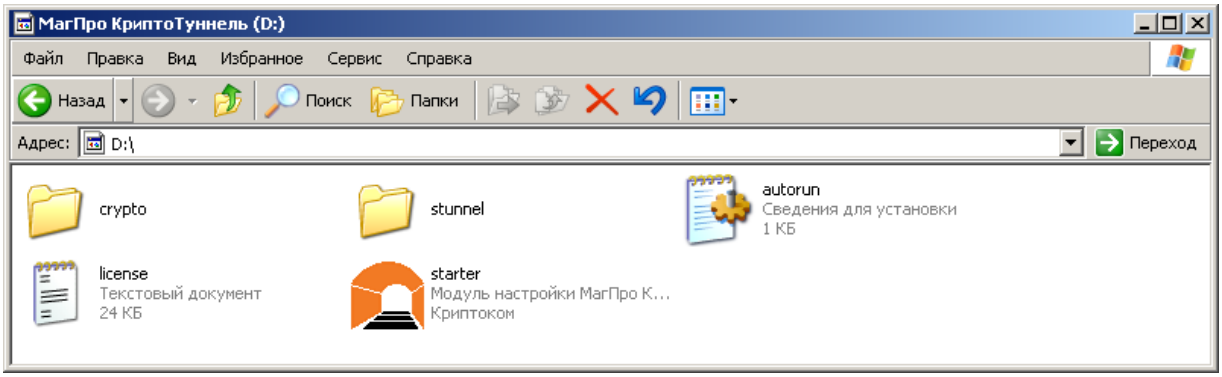
Если на компьютере включен autorun, то подключении носителя программный комплекс запускается автоматически.

Если autorun не включен, необходимо запустить ПК «МагПро КриптоТуннель» через окно «Мой компьютер». Для этого необходимо:

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



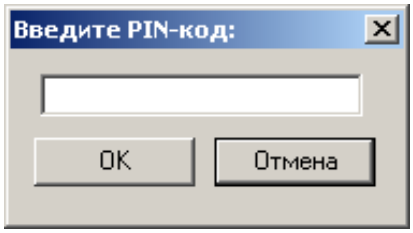
2. Запустить ПК «МагПро КриптоТуннель», дважды щелкнув мышью по иконке starter:



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

7.2 Ввод PIN-кода

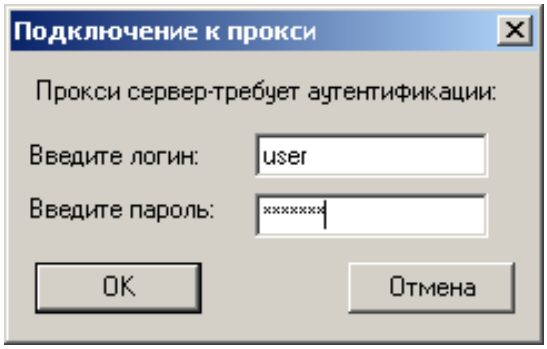
Если закрытый ключ пользователя защищен PIN-кодом, то после запуска ПК «МагПро КриптоТуннель» выводится окно запроса PIN-кода ключа:



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

7.3 Работа через прокси-сервер

Если пользователь использует прокси-сервер, требующий аутентификации, то при запуске ПК «МагПро 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.

ПК «МагПро 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 ПК «МагПро КриптоТуннель» всегда выбирает NTLM, т.е. необходимо вводить доменный логин и пароль.

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.

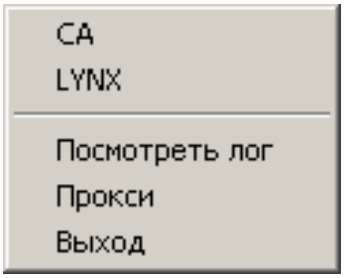
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7.4 Контекстное меню

Контекстное меню ПК «МагПро КриптоТуннель» появляется при щелчке правой клавишей мыши на иконке ПК «МагПро 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 8.3), «Прокси» (см. раздел 6.5) и «Выход» (см. раздел 9).

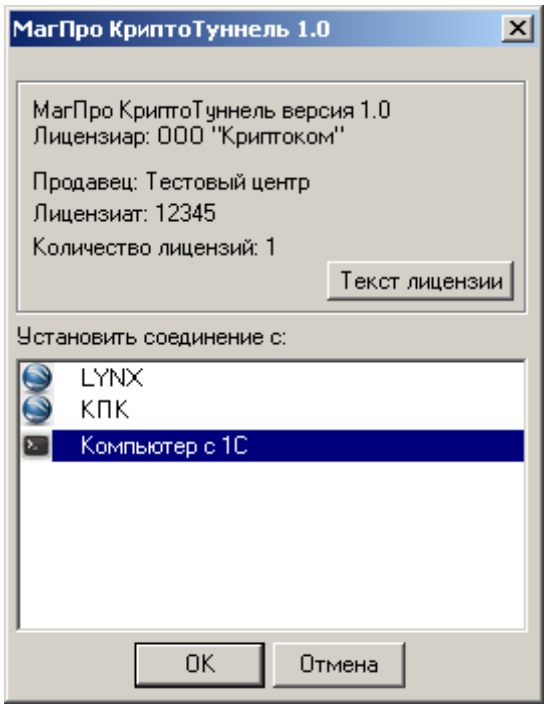
Пример контекстного меню:



8 ВЫПОЛНЕНИЕ ПРОГРАММЫ

8.1 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:



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.

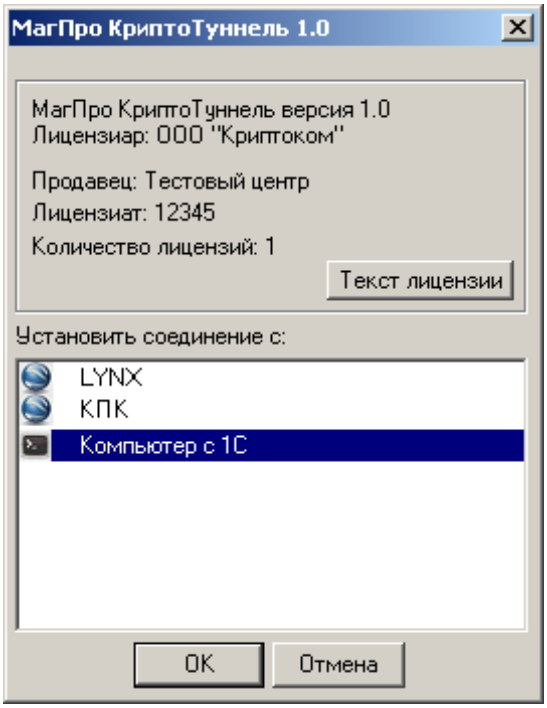
Следует щелкнуть мышью по названию необходимого объекта и нажать на кнопку «Ок». Будет установлено защищенное соединение с выбранным объектом. Если выбрано https-соединение, то запускается браузер, в котором открывается необходимая пользователю страница; если выбрано rdp-соединение, то открывается окно,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

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

Установить соединение с сайтом в этом случае можно двумя способами:

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

– Либо дважды щелкнуть левой клавишей мыши по иконке ПК «МагПро 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 ПК «МагПро КриптоТуннель» 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.

– Либо щелкнуть правой кнопкой мыши по иконке ПК «МагПро 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 ПК «МагПро КриптоТуннель» в трее, всплывает комментарий, содержащий техническую информацию о защищенном соединении: название работающего ПК, 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 КриптоТуннель 1.0
ca.cryptocom.ru:443 GOST
```

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

Если в конфигурационном файле указан только один объект для установления удаленного соединения, то при запуске ПК «МагПро 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.*

8.2 Электронная цифровая подпись

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

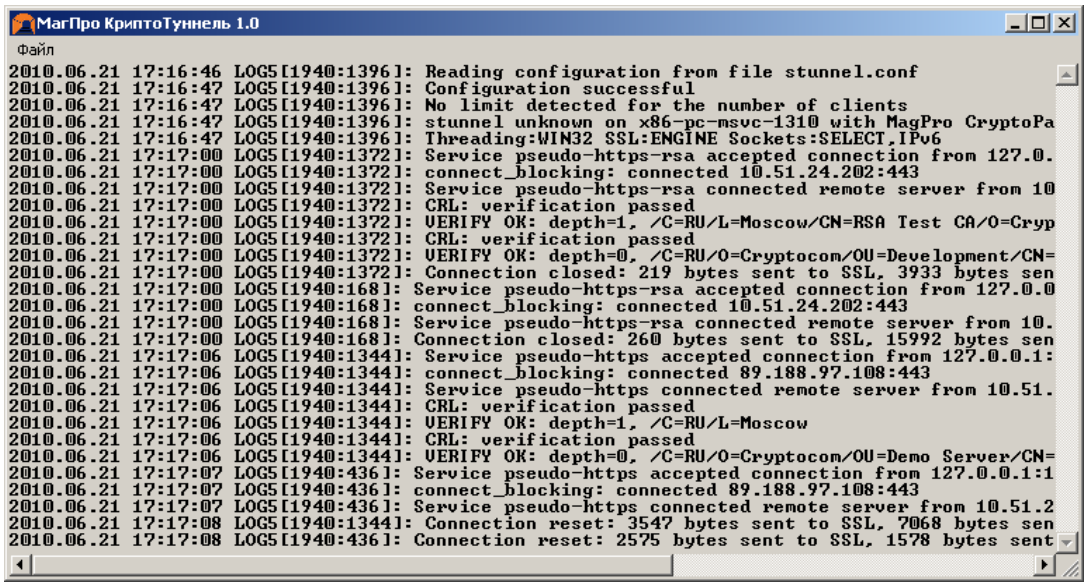
Конкретная процедура отправки онлайн-запроса или файла определяется администратором сайта. Подписывание данных может быть автоматическим или после подтверждения пользователем.

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

8.3 Журнал работы ПК КриптоТуннель

Журнал работы ПК «МагПро КриптоТуннель» содержит информацию о всех операциях, выполненных ПК «МагПро КриптоТуннель» с момента последнего запуска. Эта информация может быть полезна для системного администратора при возникновении каких-либо ошибок при работе ПК «МагПро КриптоТуннель» (см. раздел 10).

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



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

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.

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

9 ВЫХОД ИЗ ПРОГРАММЫ

Для выхода из программы необходимо:

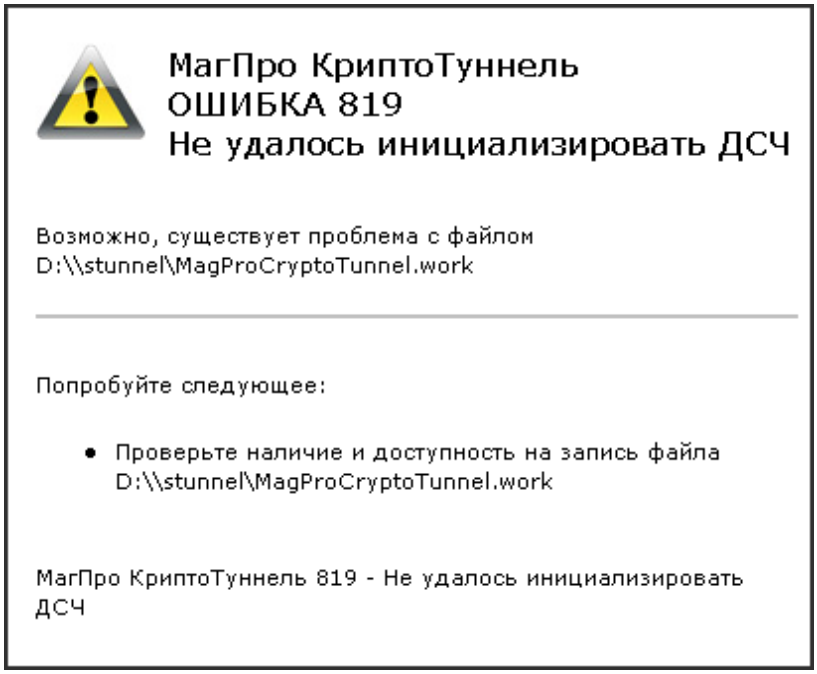
1. Щелкнуть правой клавишей мыши по иконке ПК «МагПро КриптоТуннель» в трее (в правой нижней части экрана);
2. В появившемся контекстном меню щелкнуть левой кнопкой мыши по пункту «Выход».

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

10 СООБЩЕНИЯ ОПЕРАТОРУ

10.1 Общие замечания

Если при работе ПК «МагПро КриптоТуннель» 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 ПК «МагПро КриптоТуннель».

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

10.2 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 МагПро 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 МагПро 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 МагПро 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 МагПро КриптоТуннель, в каталог crypto.
825	Возможно, сервер требует клиентской аутентификации, а в МагПро КриптоТуннель не указан сертификат клиента	Сервер требует клиентской аутентификации	Внесите исправления в конфигурационный файл stunnel.conf, как описано в разделе 6.3.
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 МагПро 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 МагПро 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 МагПро 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 МагПро КриптоТуннель, в каталог crypto.

10.3 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	МагПро 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

10.4 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 ПК «МагПро КриптоТуннель», 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 ПК «МагПро КриптоТуннель», 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 ПК «МагПро КриптоТуннель», 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 ПК «МагПро КриптоТуннель», и попросите оформить для вас новый файл лицензии в соответствии с условиями лицензирования

10.5 Предупреждение о скором окончании срока действия лицензии

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

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

10.6 Всплывающие сообщения

Сообщения, всплывающие над иконкой ПК «МагПро КриптоТуннель» 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 ПК «МагПро КриптоТуннель»	Обратитесь к лицу, от которого вы получили ПК «МагПро КриптоТуннель»
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.

11 ПРИЛОЖЕНИЯ

11.1 Файлы сертификатов

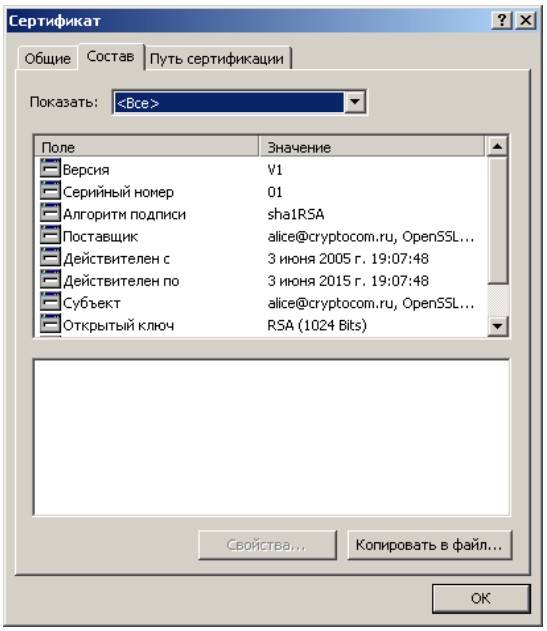
11.1.1 Файл сертификатов УЦ

Для работы ПК «МагПро КриптоТуннель» 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).

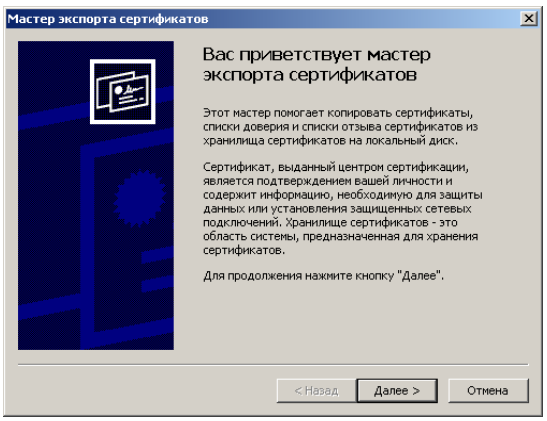
Сертификаты в этом файле должны быть в формате PEM. Если сертификат УЦ получен в формате DER (расширения .cer или .crt) или PKCS#7 (расширение p7b), то можно воспользоваться системными средствами Windows для конвертации его в формат PEM.

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

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



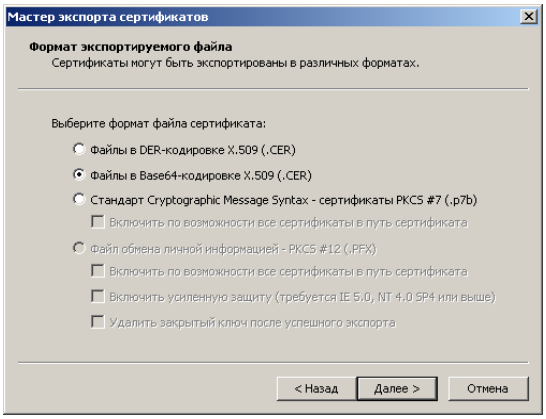
2. Нажать на кнопку «Копировать в файл». Запустится мастер экспорта сертификатов;



Нажать на кнопку «Далее».

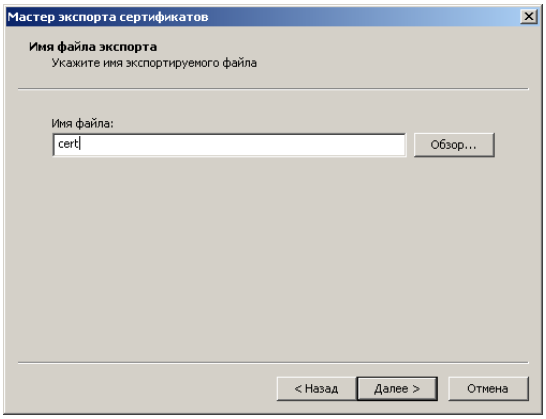
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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

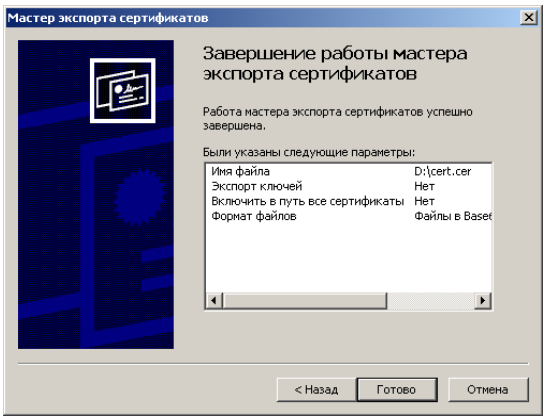


и нажать на кнопку «Далее»;

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



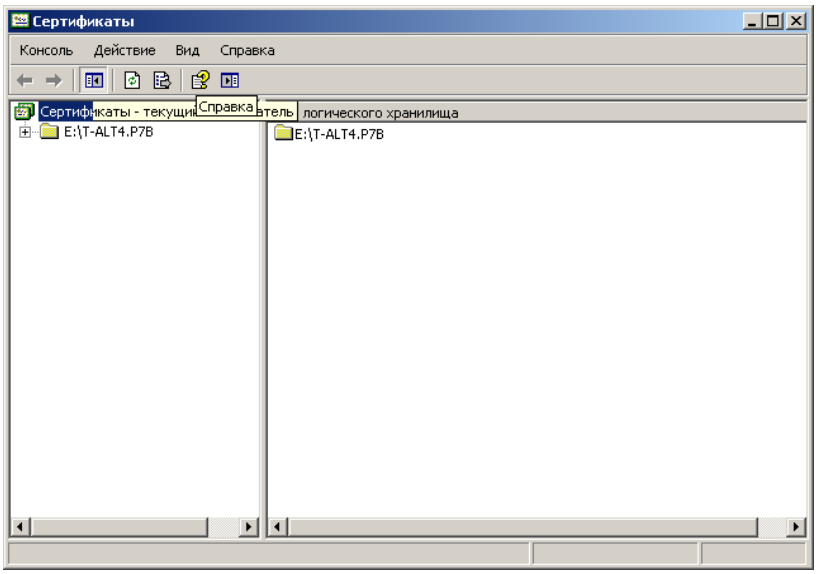
5. Нажать на кнопку «Готово».



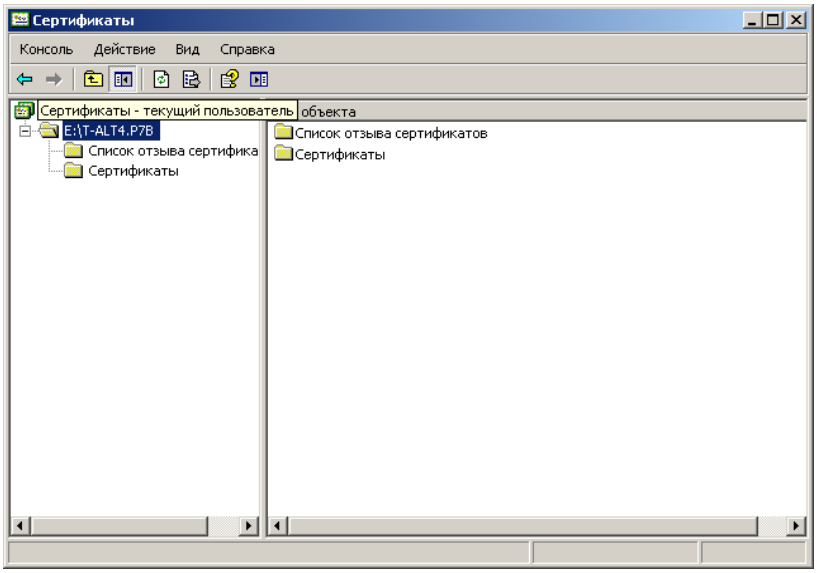
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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

1. Двойным щелчком мыши открыть окно просмотра цепочки сертификатов:

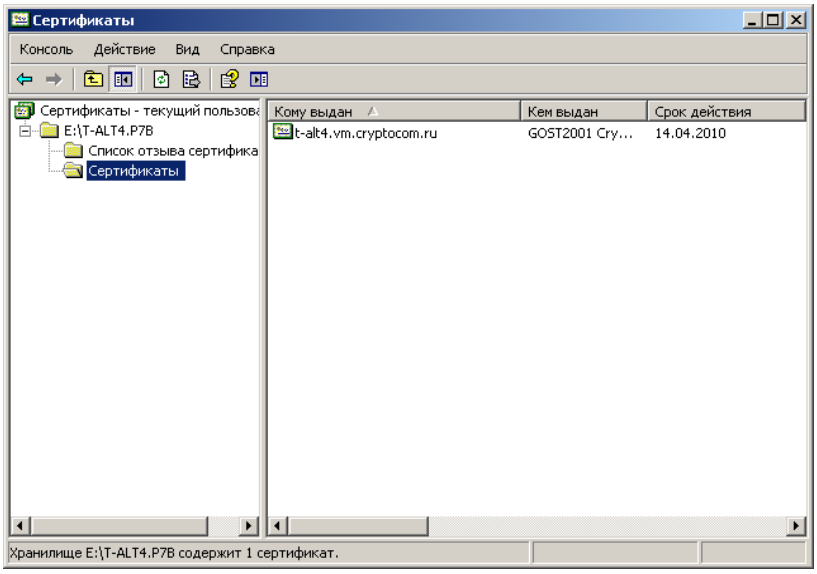


2. Щелчком мыши по наименованию цепочки сертификатов раскрыть ее содержание:



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 ПК «МагПро КриптоТуннель».

11.1.2 Ограничение на самоподписанные сертификаты серверов

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

11.1.3 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 6.3.

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

11.2 Адреса страниц, приводящие к разрыву https-соединения

Когда пользователь, установив защищенное соединение с сервером с помощью ПК «МагПро КриптоТуннель», переходит по внутренним ссылкам на другие страницы на этом сервере, в большинстве случаев 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.

11.2.1 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://[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 удаленном сайте должны быть относительными.

11.2.2 Адреса каталогов

Если пользователь переходит по ссылке на каталог, то для сохранения HTTPS-соединения ссылка на каталог должна обязательно заканчиваться знаком /. Если этого знака нет, сервер выполняет редирект на адрес со знаком / по протоколу HTTPS, в результате чего также происходит попытка установить новое HTTPS-соединение напрямую. Т.к. сам браузер не может работать с алгоритмами GOST, такое соединение установить не удается.

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