КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00018-01 33 01 - ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС
МагПро КриптоСервер вер. 1.0

Руководство системного администратора

СЕИУ.00018-01 33 01
Листов 12

Литера О

2010

Аннотация

Настоящий документ содержит руководство системного администратора сервера для работы с ПК «МагПро КриптоСервер» 1.0.

Содержание

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

1 ВВЕДЕНИЕ

1.1 Назначение программного комплекса

ПК «МагПро КриптоСервер» 1.0 позволяет подготовить сервер IIS для установления соединений, защищенных по протоколу TLS (HTTPS-соединение), с использованием алгоритмов ГОСТ.

ПК «МагПро КриптоСервер» 1.0 является сертифицированным решением для установления защищенного https-соединения клиентов, использующих ПК МагПро КриптоТуннель, с сервером, на котором установлен ПК «МагПро КриптоСервер» 1.0, с использованием алгоритмов ГОСТ. (С помощью ПК «МагПро КриптоСервер» 1.0 можно устанавливать https-соединение и с использованием других алгоритмов, но в таком случае это будет несертифицированное решение.)

1.2 Условия работы программного комплекса

ПК «МагПро КриптоСервер» 1.0 предназначен для работы в ОС Windows 2000/2000 Server/XP/2003 Server/Vista/Windows 7/2008 Server.

Сервер IIS необходимо перенастроить так, чтобы он принимал соединения только на localhost. Если этого не сделать, не будут исключены незащищенные соединения (по протоколу http), причем пользователь не получит информации о том, какое именно соединение установлено.

Сервер, с которым предполагается устанавливать защищенные соединения, должен соответствовать определенным требованиям (см. раздел 4.1).

1.3 Лицензирование

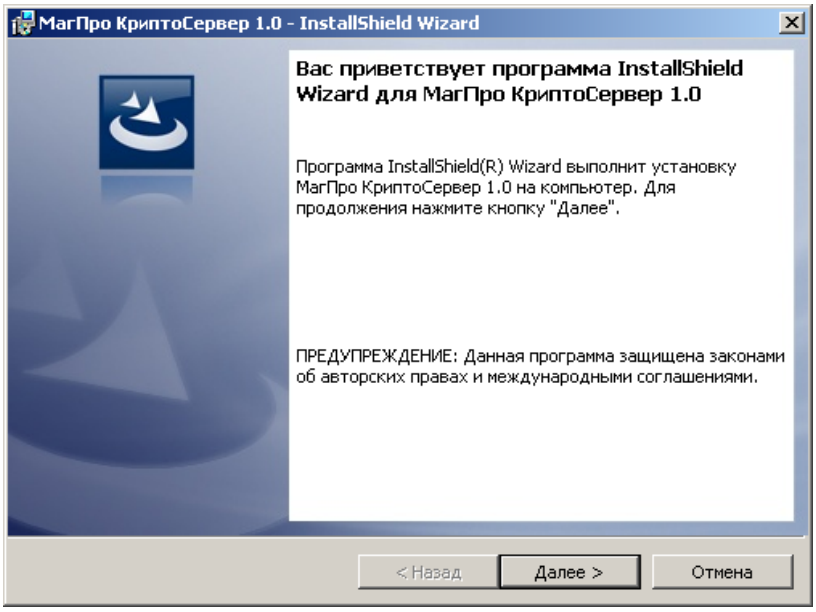
Лицензия на ПК «МагПро КриптоСервер» 1.0 выдается сроком на 1 год.

По окончании срока действия лицензии ПК «МагПро КриптоСервер» 1.0 прекращает работу. Чтобы продолжить работу с ПК «МагПро КриптоСервер» 1.0 после окончания срока действия лицензии, необходимо получить у производителя дистрибутив ПК «МагПро КриптоСервер» 1.0 с новой лицензией и установить его на сервере.

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

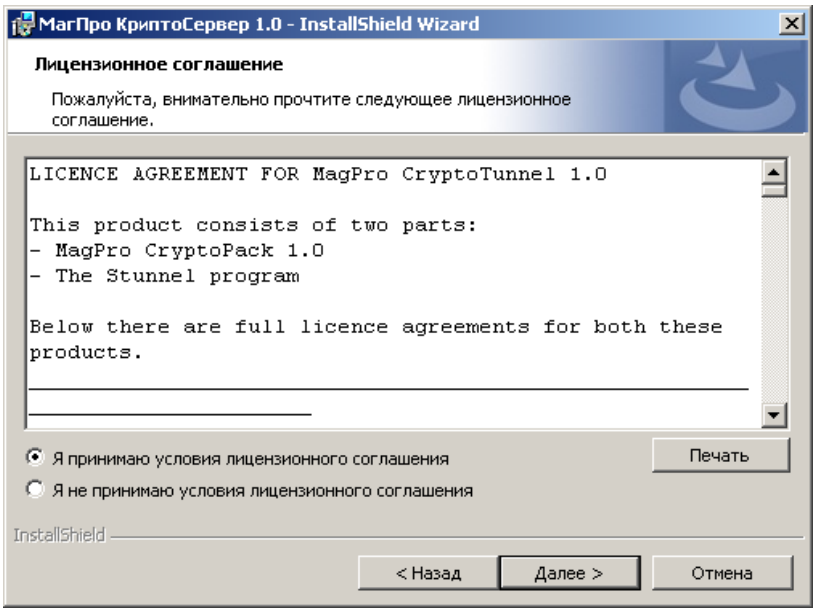
2 УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

1. Запустить пакет инсталляции magpro-cryptoserver-1.0.



Нажать на кнопку «Далее».

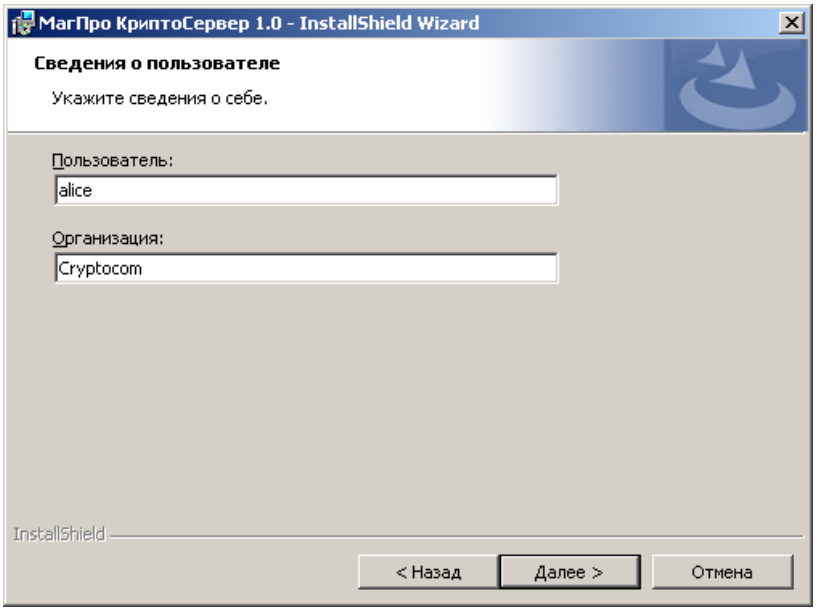
2. Выводится окно лицензионного соглашения. Прочесть его и при согласии выбрать «Я принимаю условия лицензионного соглашения»:



Нажать на кнопку «Далее».

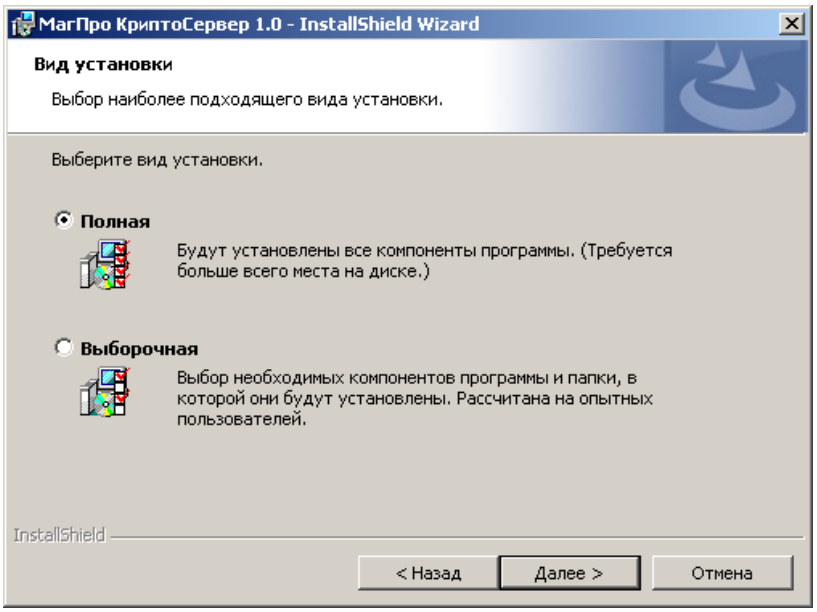
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Указать сведения о себе и об организации.



Нажать на кнопку «Далее».

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

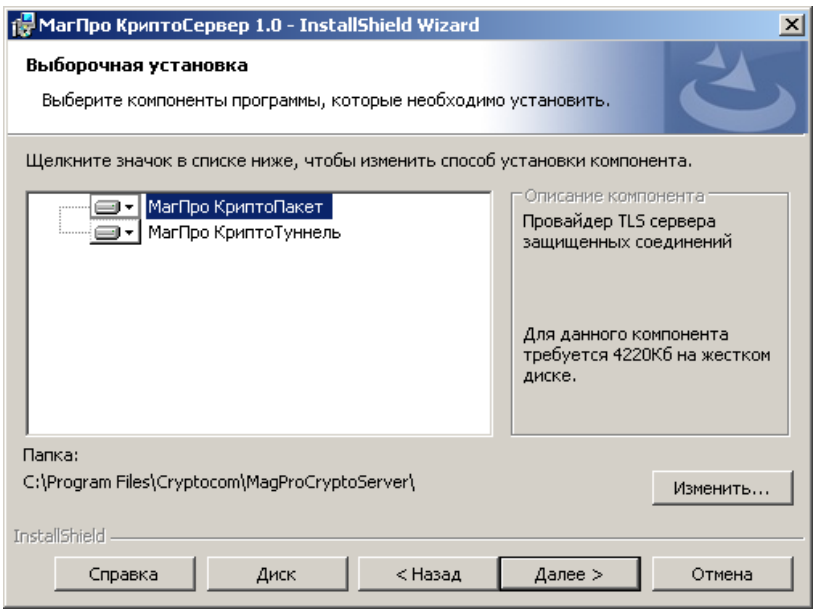


В ПК «МагПро КриптоСервер» 1.0 нет компонентов, которые можно исключить из установки, но на странице выборочной установки можно изменить установочный каталог, заданный по умолчанию.

Выбрав вид установки, нажать на кнопку «Далее».

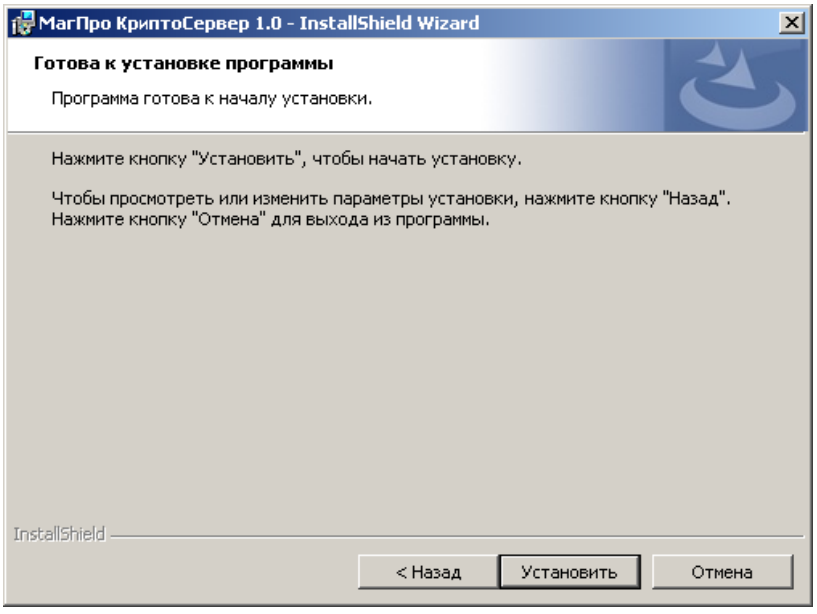
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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».

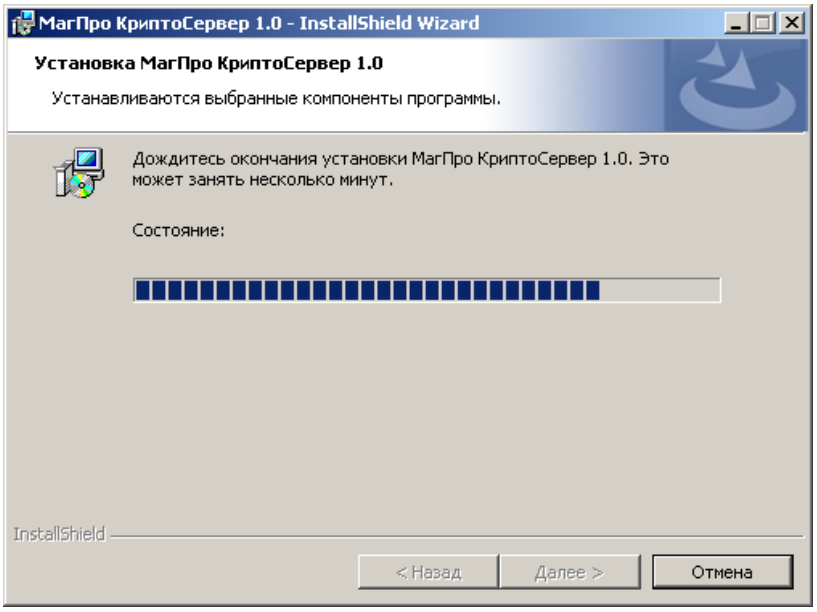
6. Выводится окно, сообщающее о готовности программы к установке.



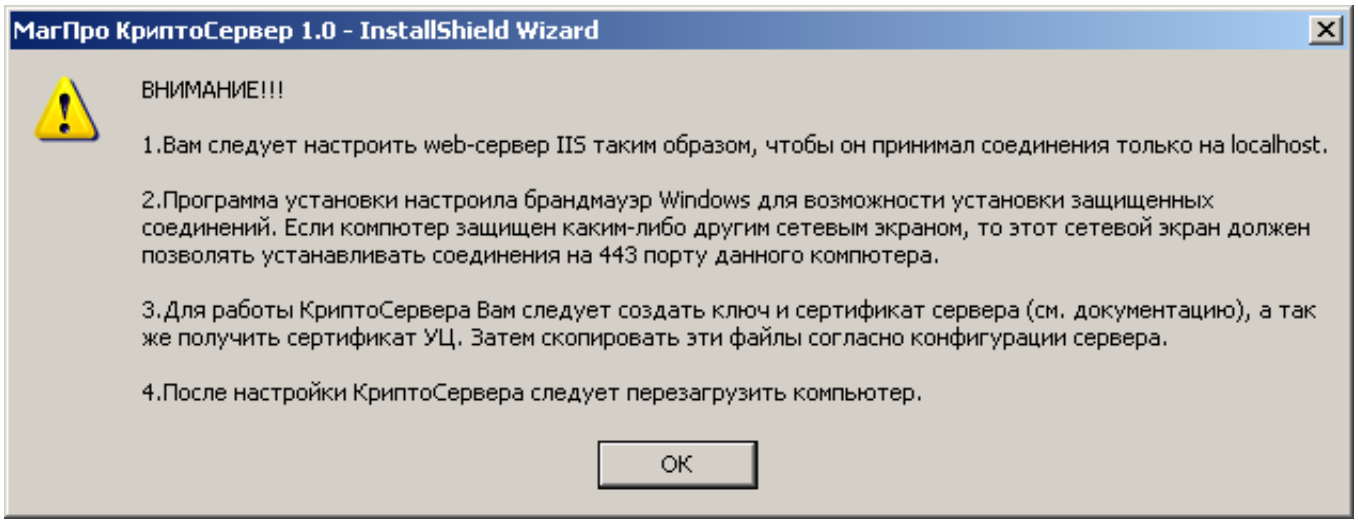
Нажать на кнопку «Далее».

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

7. Выводится окно, отражающее процесс установки:



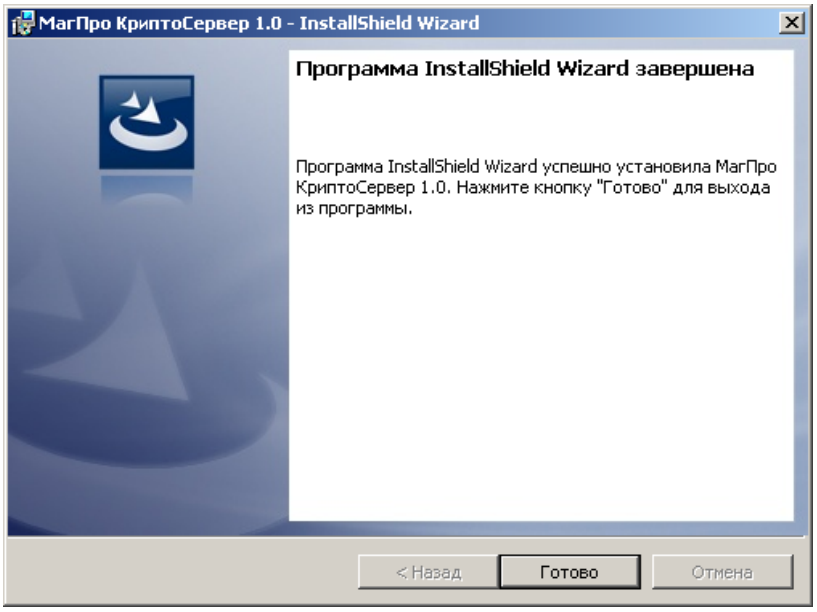
8. Во время установки выводится окно, содержащее важные предупреждения:



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 ПК «МагПро КриптоСервер» 1.0:



Нажать на кнопку «Готово».

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

3 КЛЮЧЕВАЯ ИНФРАСТРУКТУРА

3.1 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 ПК «МагПро КриптоСервер» 1.0 (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)*.

3.2 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)*.

3.3 Формат файлов ключевой информации

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

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

4 ПРИЛОЖЕНИЕ

4.1 Адреса страниц, приводящие к разрыву https-соединения

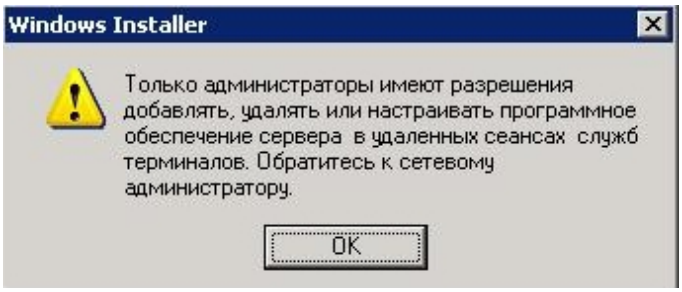
Когда пользователь, установив защищенное соединение с сервером с помощью ПК «МагПро КриптоСервер» 1.0, переходит по внутренним ссылкам на другие страницы на этом сервере, в большинстве случаев соединение остается защищенным. Но в некоторых случаях происходит переход к незащищенному соединению. Это связано с форматом, в котором во внутренних ссылках на сервере указаны адреса страниц, на которые переходит пользователь.

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.

4.2 Установка по RDP

Как правило, установка ПК «МагПро КриптоСервер» 1.0 в RDP-сессии не представляет сложностей.

Если на сервере установлена роль «Сервер терминалов», возможность установки ПК «МагПро КриптоСервер» 1.0 по RDP связана с локальной и доменной политиками «Локальный компьютер — Административные шаблоны — Компоненты Windows — Установщик Windows — Разрешить администраторам выполнение установки в сеансе сервера терминалов». Если эти политики не определены, возможно появление следующей ошибки:



В этом случае следует:

1. Убедиться, что на сервере установлена роль «Сервер терминалов»;
2. Если установлена, явным образом установить локальную и доменную политики «Локальный компьютер — Административные шаблоны — Компоненты Windows — Установщик Windows — Разрешить администраторам выполнение установки в сеансе сервера терминалов».
3. Повторить установку ПК «МагПро КриптоСервер» 1.0.

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

Лист регистрации изменений

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

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