

УТВЕРЖДЕН
СЕИУ.00019-01 33 01 - ЛУ

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

ПРОГРАММНЫЙ КОМПЛЕКС
МагПро КриптоПортал вер. 1.0
Руководство системного администратора сервера
СЕИУ.00019-01 33 01
Листов 13

Литера О

Аннотация

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

Авторские права на ПК «МагПро КriptoПортал» 1.0 принадлежат ООО «Кriptoком».

В коде ПК использован код OpenSSL, ©1998-2004, The OpenSSL Project, и код программы stunnel by Michal Trojnara, <http://www.stunnel.org>.

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

Содержание

1 ВВЕДЕНИЕ	4
1.1 Назначение программного комплекса	4
1.2 Условия работы программного комплекса	4
2 УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА	5
3 ПРИЛОЖЕНИЕ	12
3.1 Адреса страниц, приводящие к разрыву https-соединения	12
3.2 Установка по RDP	12

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

1 ВВЕДЕНИЕ

1.1 Назначение программного комплекса

ПК «МагПро КриптоПортал» 1.0 позволяет установить соединение клиента с сервером, защищенное по протоколу TLS (HTTPS-соединение), с использованием алгоритмов ГОСТ, с предварительной автоматической процедурой создания сертификатов и ключей сервера и клиента.

ПК «МагПро КриптоПортал» 1.0 является сертифицированным решением для установления защищенного https-соединения клиентов, использующих пользовательский комплект, с сервером, на котором установлен серверный комплект, с использованием алгоритмов ГОСТ.

ПК «МагПро КриптоПортал» 1.0 при установке создает и устанавливает все необходимые сертификаты для сервера, а также создает готовый к работе клиентский пользовательский комплект. Данный пользовательский комплект необходимо скопировать на носители (flash-носители, лазерные диски) и раздать пользователям, которые будут устанавливать защищенное соединение с данным сервером.

При установлении защищенного соединения ПК «МагПро КриптоПортал» 1.0 устанавливает соединение только с пользовательскими комплектами, созданными с помощью данного экземпляра ПК «МагПро КриптоПортал» 1.0.

1.2 Условия работы программного комплекса

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

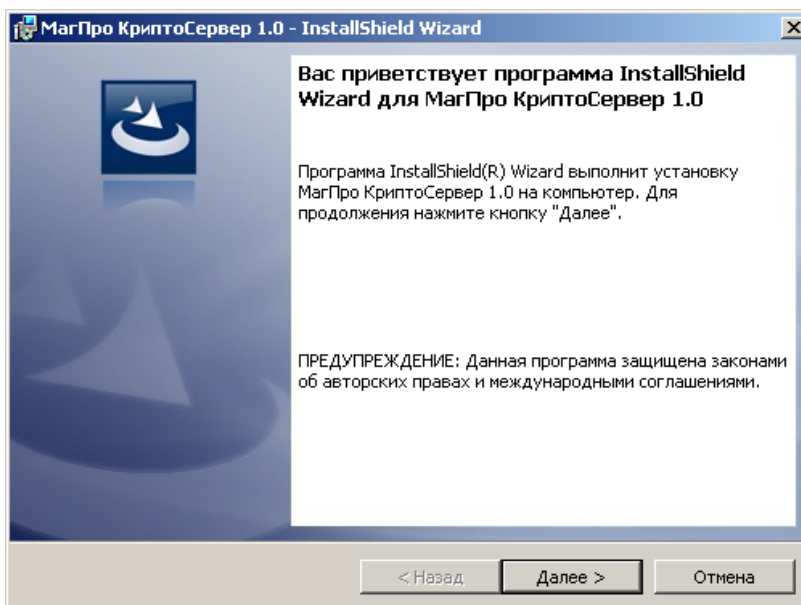
Сервер IIS необходимо перенастроить так, чтобы он принимал соединения только на localhost. Если этого не сделать, не будут исключены незащищенные соединения (по протоколу http), причем пользователь не получит информации о том, какое именно соединение установлено.

Сервер, с которым предполагается устанавливать защищенные соединения, должен соответствовать определенным требованиям (см. раздел 3.1).

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

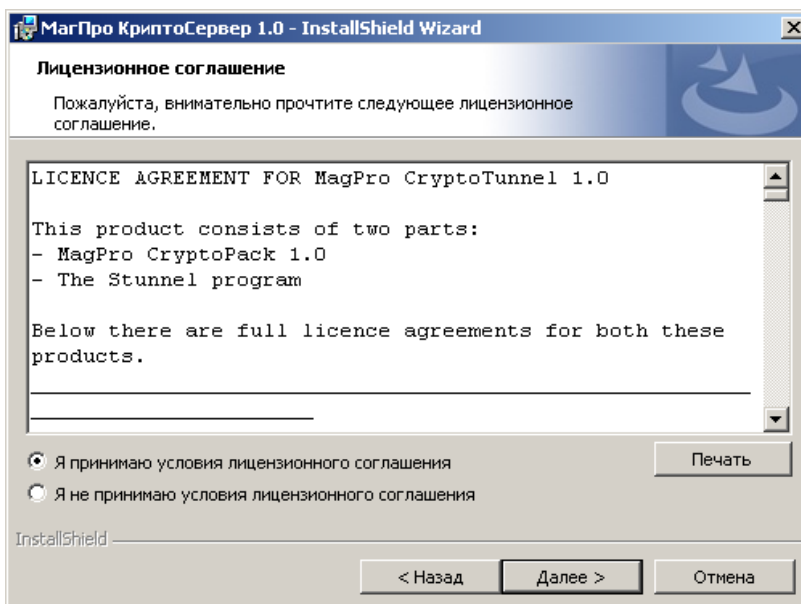
2 УСТАНОВКА ПРОГРАММНОГО КОМПЛЕКСА

1. Запустить пакет инсталляции magpro-cryptoserver-1.0.



Нажать на кнопку «Далее».

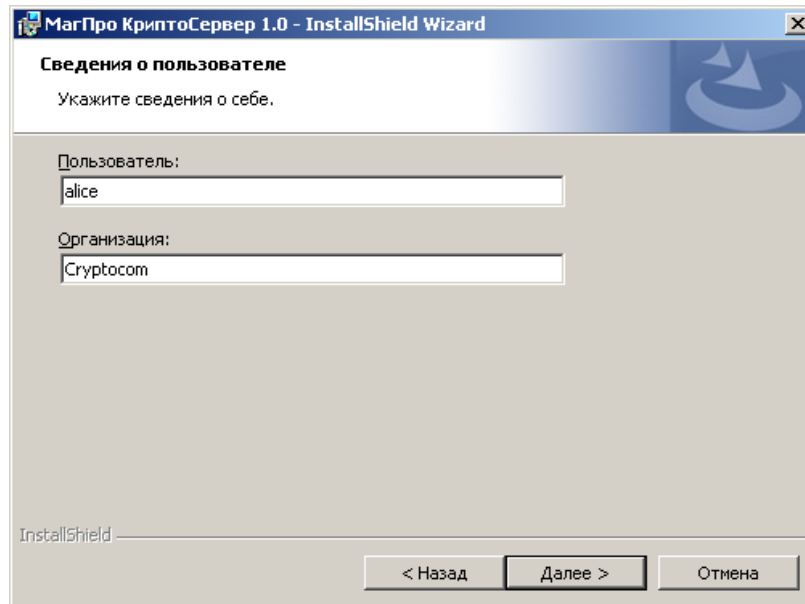
2. Выводится окно лицензионного соглашения. Прочсть его и при согласии выбрать «Я принимаю условия лицензионного соглашения»:



Нажать на кнопку «Далее».

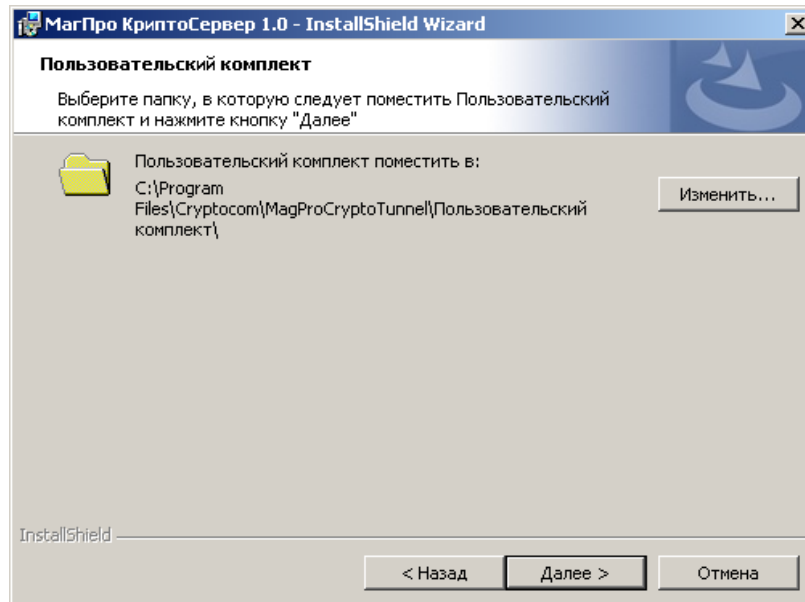
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3. Указать сведения о себе и об организации.



Нажать на кнопку «Далее».

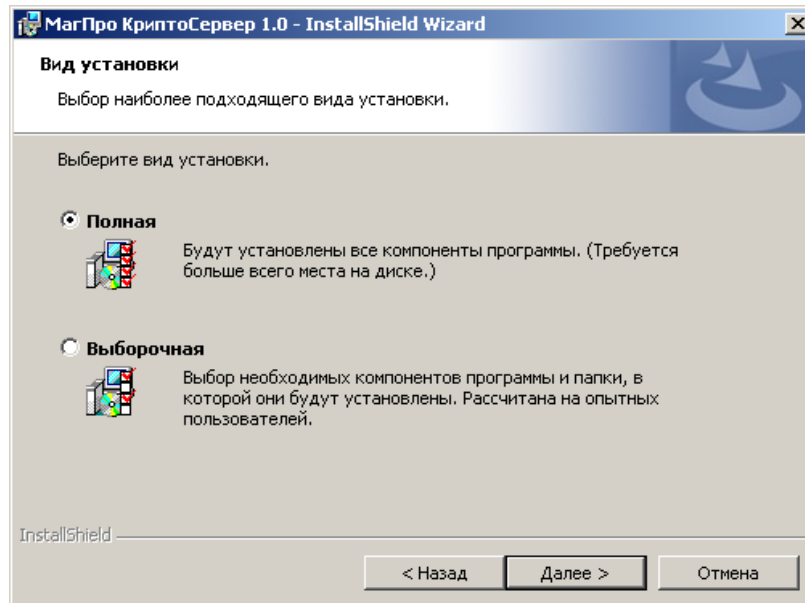
4. Выбрать каталог, в котором будет создан пользовательский комплект. Можно оставить каталог, указанный по умолчанию, или выбрать другой с помощью кнопки «Изменить». Если указанного каталога не существует, инсталлятор его создаст:



Нажать на кнопку «Далее».

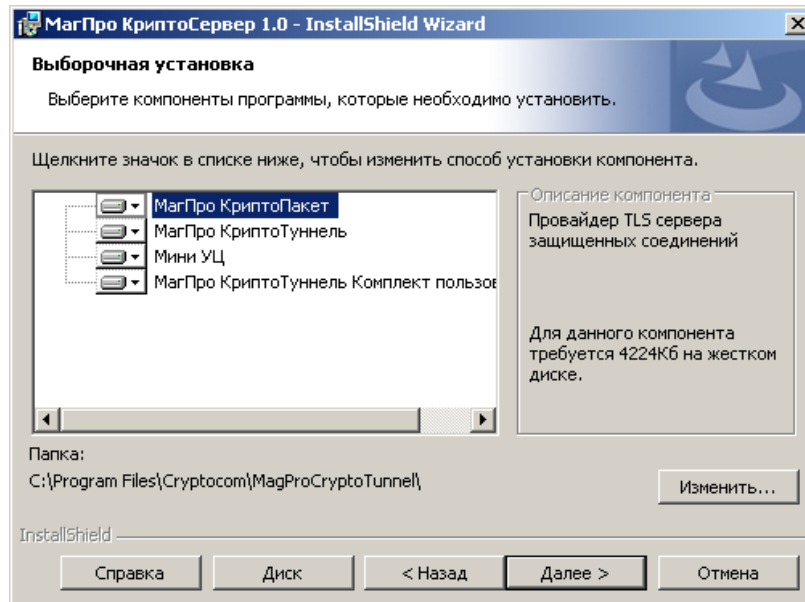
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5. Выводится окно выбора вида установки — полная или выборочная. Рекомендуется выбирать полную установку, т.к. в ПК «МагПро КриптоПортал» 1.0 нет компонентов, которые можно исключить из установки:



Выбрав вид установки, нажать на кнопку «Далее».

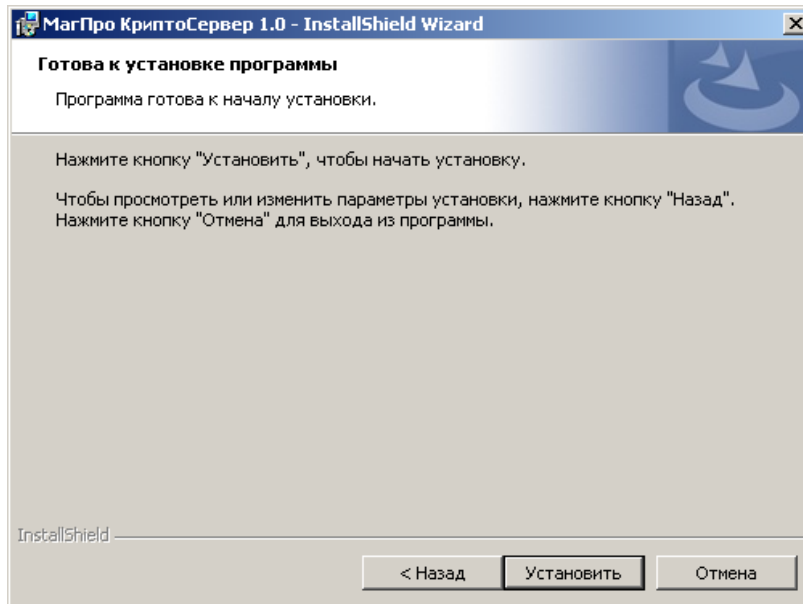
6. Если на предыдущем шаге указана выборочная установка, выводится окно выбора компонентов:



Нажать на кнопку «Далее».

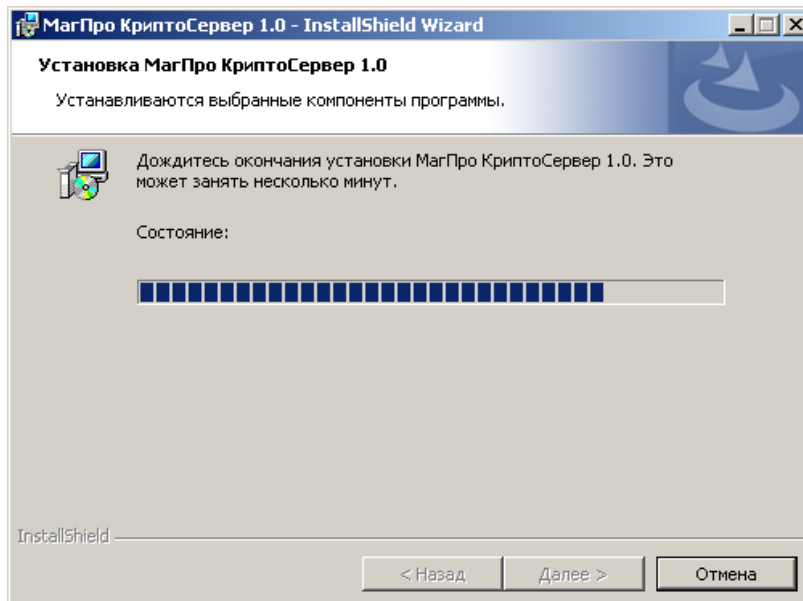
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

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



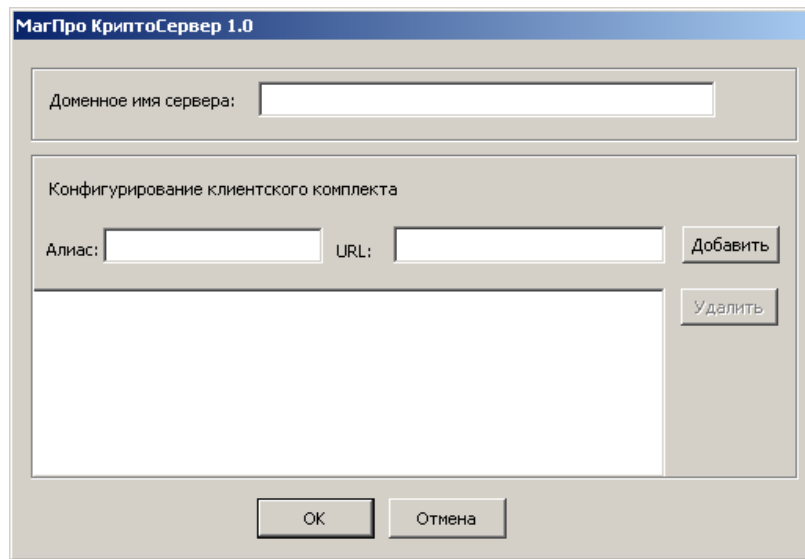
Нажать на кнопку «Далее».

8. Выводится окно, отражающее процесс установки:



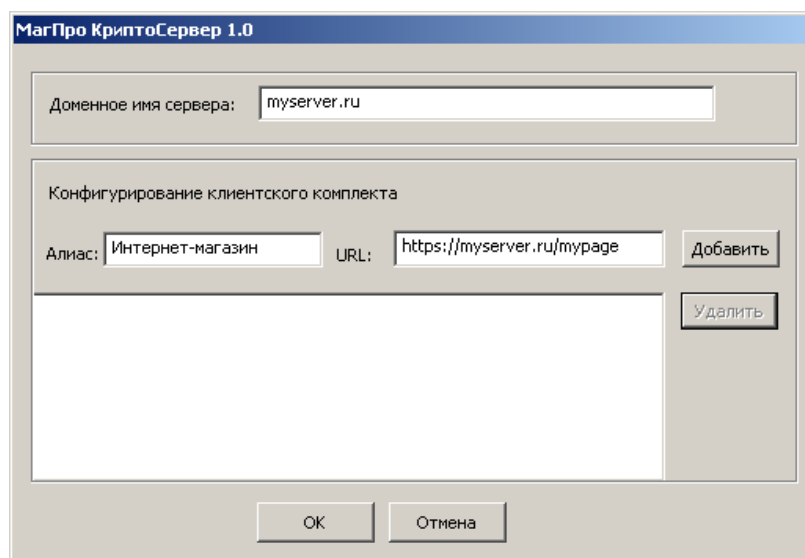
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

9. Выводится окно конфигурации пользовательского комплекта:



Заполнить поля:

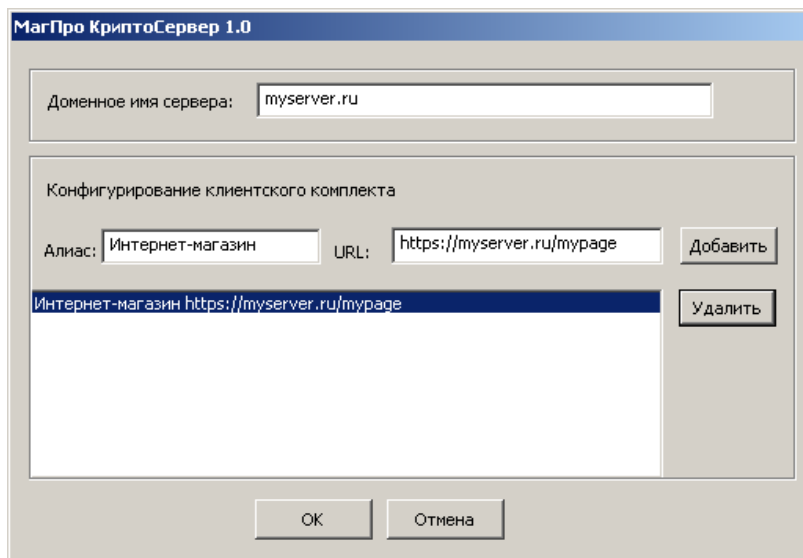
- Доменное имя сервера — указать доменное имя сервера (например myserver.ru.
- Алиас — указать удобный алиас для данного сервера, который будет использоваться клиентом при установлении соединения (например, «Интернет-магазин»)
- URL — частично автоматически заполняется при указании доменного имени сервера, возникает строка вида `https://[доменное имя]/` (например, `https://myserver.ru/`), указывающая на корневую страницу сервера. Если при соединении клиенту необходимо загрузить не корневую, а какую-либо другую страницу данного сервера, необходимо указать путь к этой странице после знака `/` (например, `https://myserver.ru/mypage.html`).



Нажать на кнопку «Добавить».

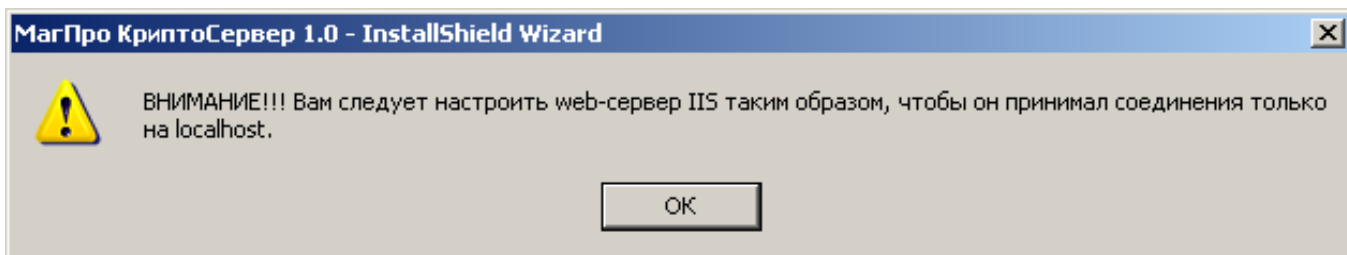
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

При этом в нижнем поле возникает строка, содержащая конфигурационную информацию для пользовательского комплекта:



Нажать на кнопку «Ок».

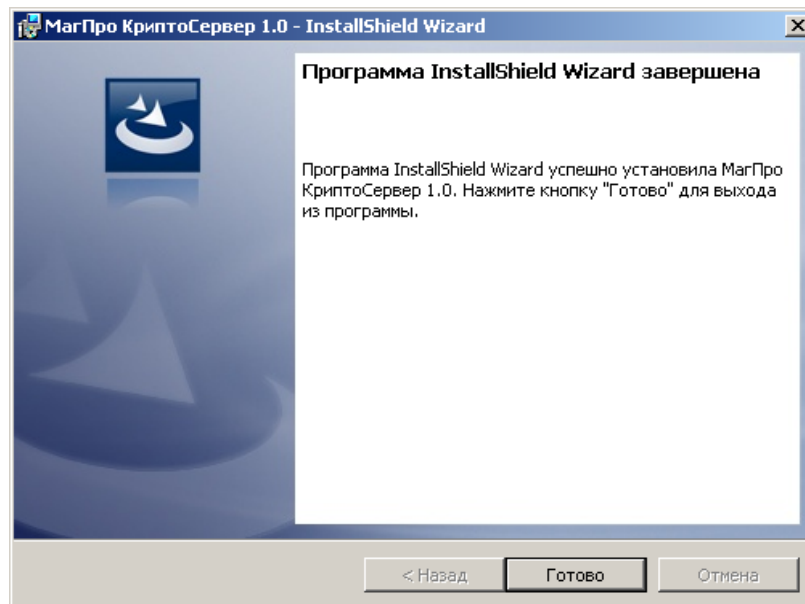
10. Выводится предупреждение:



Нажать на кнопку «Ок».

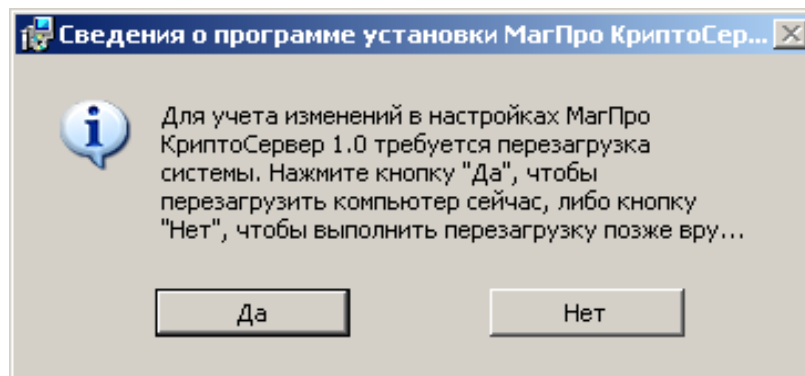
Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

11. Выводится окно с сообщением об окончании установки ПК «МагПро КриптоПортал» 1.0:



Нажать на кнопку «Готово».

12. Может быть выведено сообщение о необходимости перезагрузки системы:



Для немедленной перезагрузки системы выбрать кнопку «Да». Для того, чтобы позже перезагрузить систему вручную, выбрать кнопку «Нет».

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

3 ПРИЛОЖЕНИЕ

3.1 Адреса страниц, приводящие к разрыву https-соединения

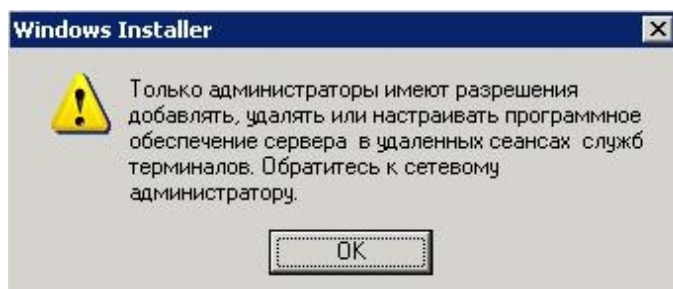
Когда пользователь, установив защищенное соединение с сервером с помощью ПК «МагПро КриптоПортал» 1.0, переходит по внутренним ссылкам на другие страницы на этом сервере, в большинстве случаев соединение остается защищенным. Но в некоторых случаях происходит переход к незащищенному соединению. Это связано 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.

3.2 Установка по RDP

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

Если на сервере установлена роль «Сервер терминалов», возможность установки ПК «МагПро КриптоПортал» 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 КриптоПортал» 1.0.

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

