127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 5.0 R2 KC1

Исполнение 1-Base

Инструкция по использованию СКЗИ под управлением ОС Windows

ЖТЯИ.00101-02 92 01
Листов 150

2021 г

Содержание

1 Инсталляция СКЗИ КриптоПро CSP

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Для установки программного обеспечения вставьте компакт-диск в дисковод (см. Рисунок 1).

Рисунок 1. Установка СКЗИ КриптоПро CSP

Выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе.

Примечание. Также установка может производиться с дистрибутива, полученного с сайта ООО «КРИПТО-ПРО». В таком случае пользователю нужно запустить файл дистрибутива CSPSetup.exe.

В начальном окне Мастера установки нажмите кнопку **Установить**, чтобы начать установку КриптоПро CSP в конфигурации КС1 и языком операционной системы (см. Рисунок 2).

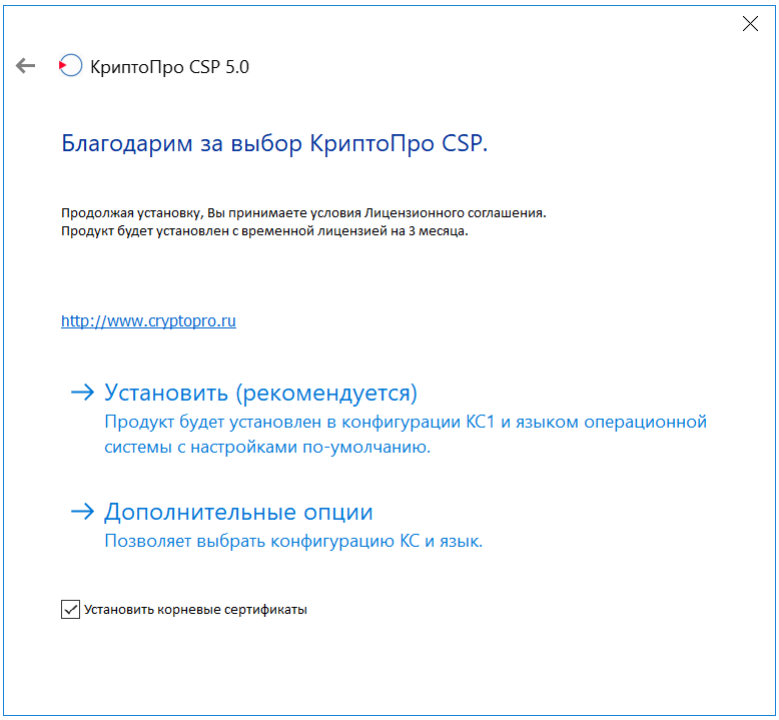


Рисунок 2. Начало установки

В СКЗИ КриптоПро CSP реализованы классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России. Для изменения конфигурации КС или языка установки нажмите кнопку **Дополнительные опции**. В открывшемся окне укажите язык установки и требуемый уровень безопасности и нажмите кнопку **Установить** (см. Рисунок 3).

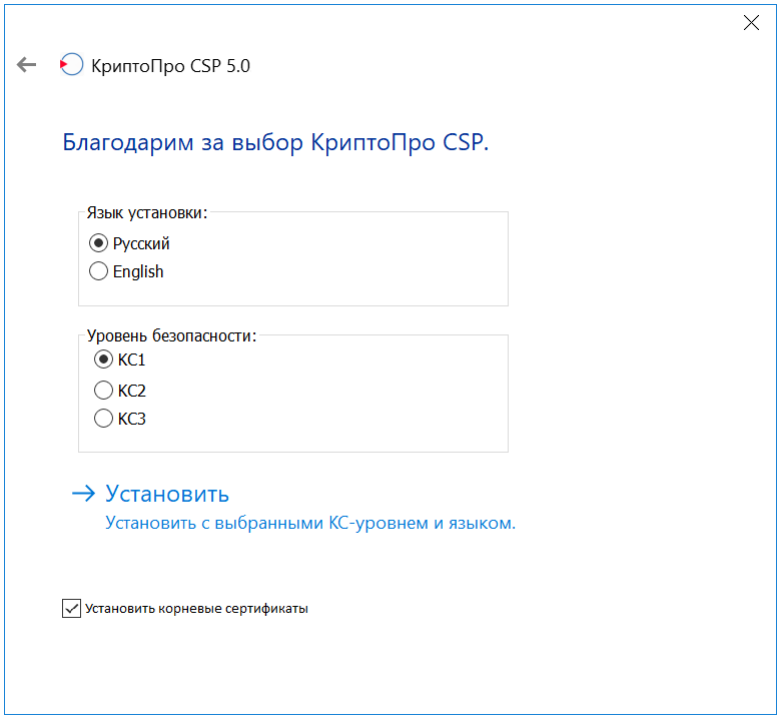


Рисунок 3. Выбор языка установки и уровня КС

Откроется Мастер установки КриптоПро CSP (КС1) (см. Рисунок 4).

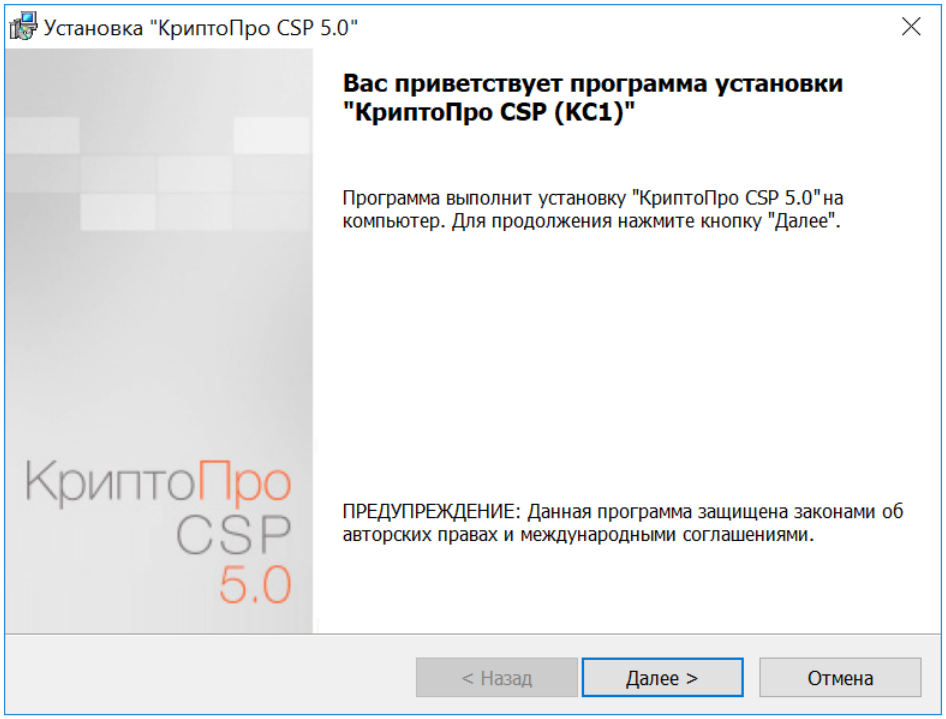


Рисунок 4. Приветственное окно Мастера установки КриптоПро CSP

Если на машине была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии (см. Рисунок 5).

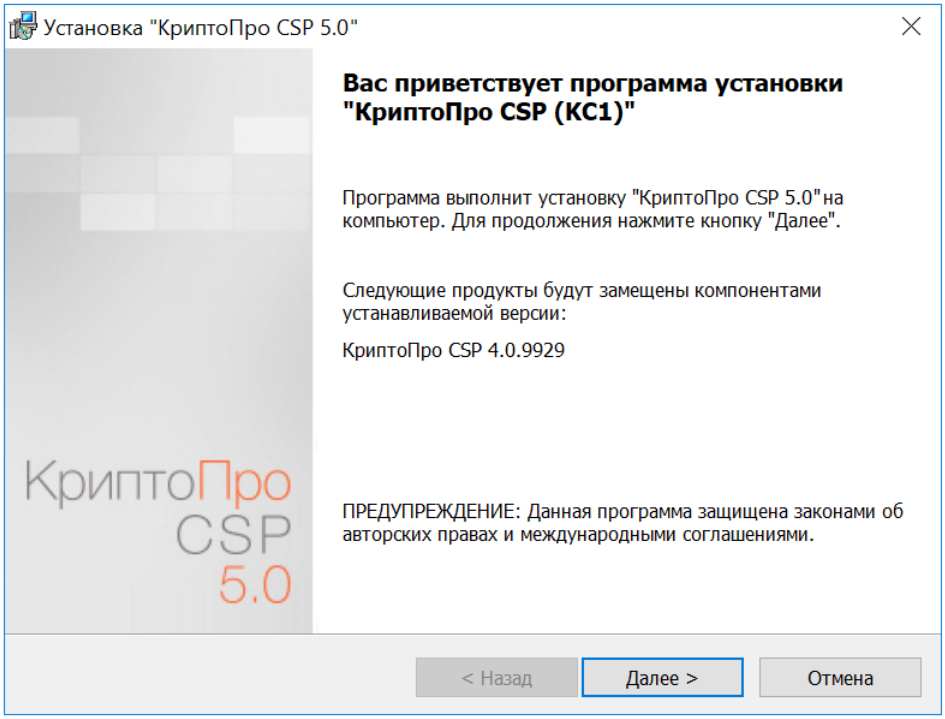


Рисунок 5. Установка КриптоПро CSP с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите кнопку **Далее**. Внимательно прочитайте лицензионное соглашение, которое выводится при первой установке (см. Рисунок 6).

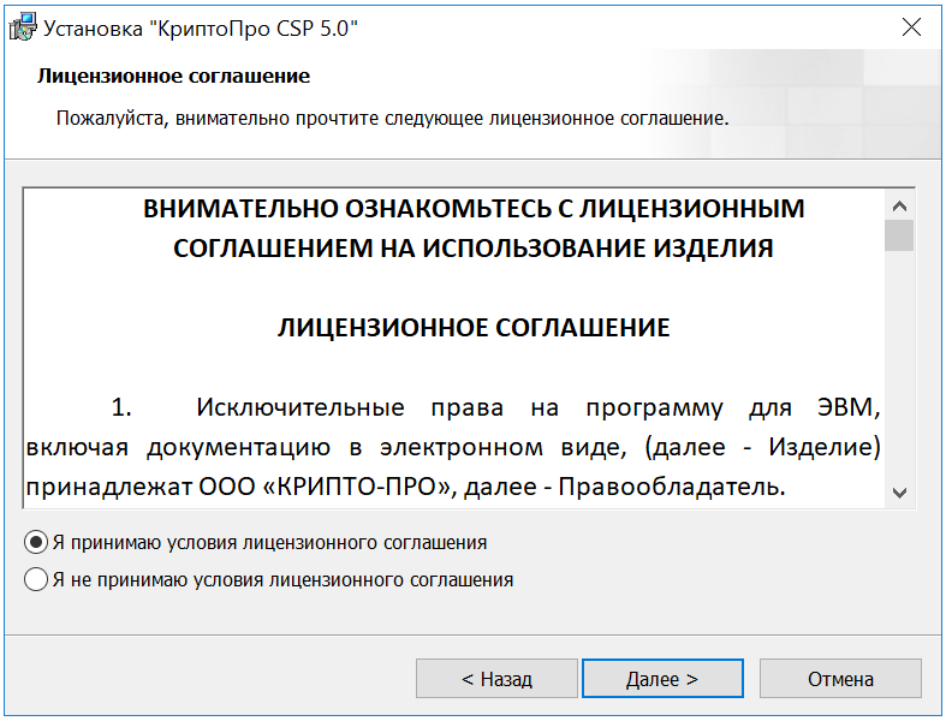


Рисунок 6. Лицензионное соглашение

В процессе установки может быть предложено:
- ввести серийный номер лицензии криптопровайдера;
- зарегистрировать дополнительные считыватели ключевой информации;
- настроить криптопровайдер на использование службы хранения ключей;

Эти параметры можно изменить после завершения установки через панель управления КриптоПро CSP.

В окне «Сведения о пользователе» заполните сведения о себе и укажите серийный номер продукта (см. Рисунок 7). Без введенного серийного номера КриптоПро CSP устанавливается с временной лицензией на 3 месяца.

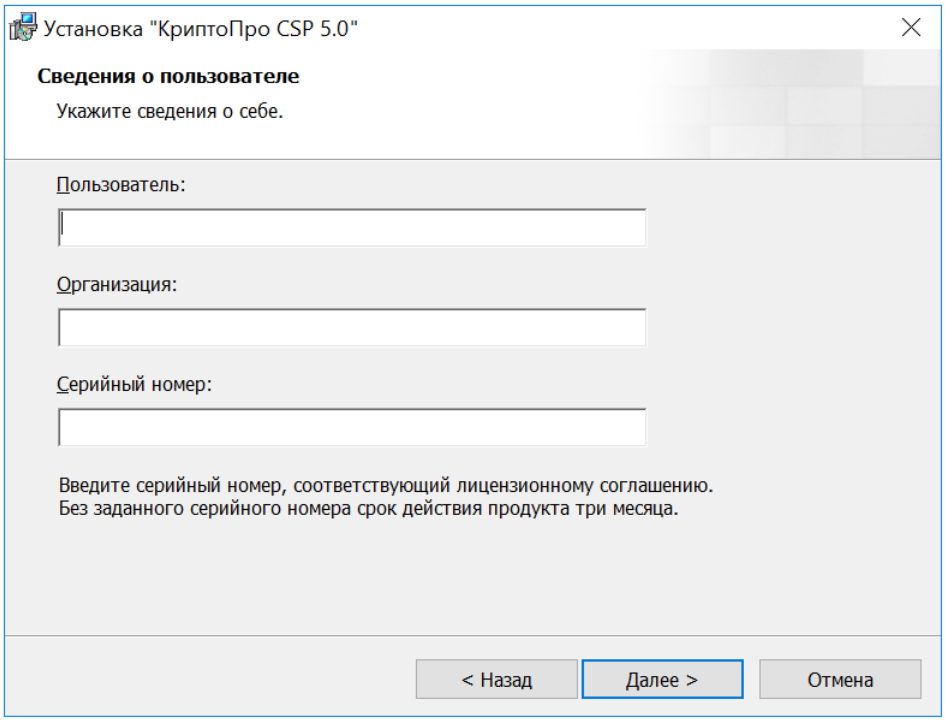


Рисунок 7. Сведения о пользователе

В окне «Вид установки» выберите подходящий вид установки КриптоПро CSP (см. Рисунок 8).

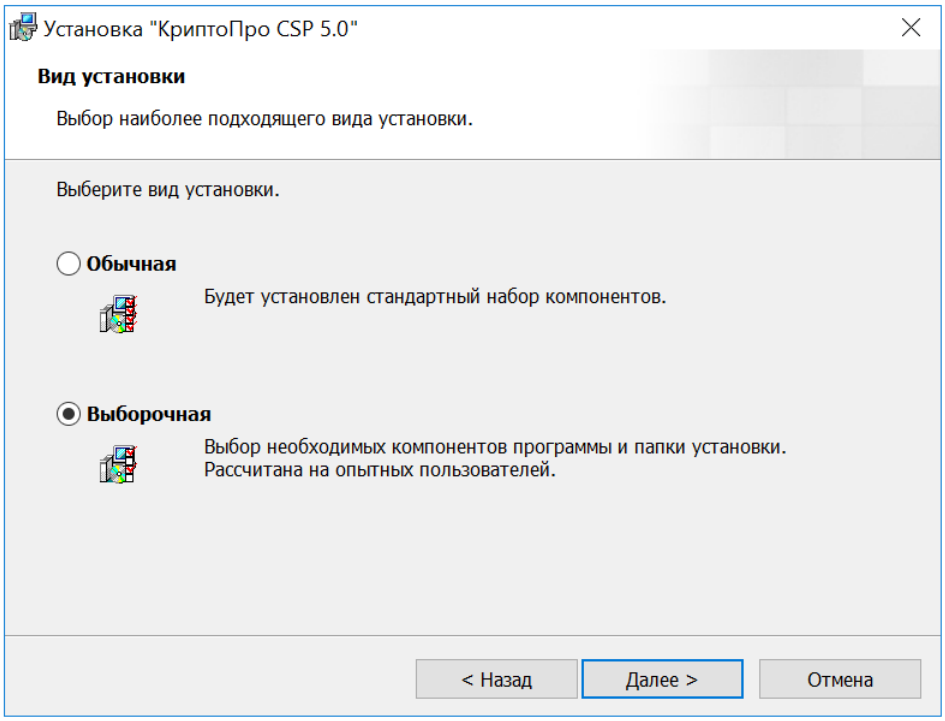


Рисунок 8. Выбор вида установки

По умолчанию (вид установки **Обычная**) устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). При необходимости (вид установки **Выборочная**) можно изменить набор компонентов для установки (см. Рисунок 9).

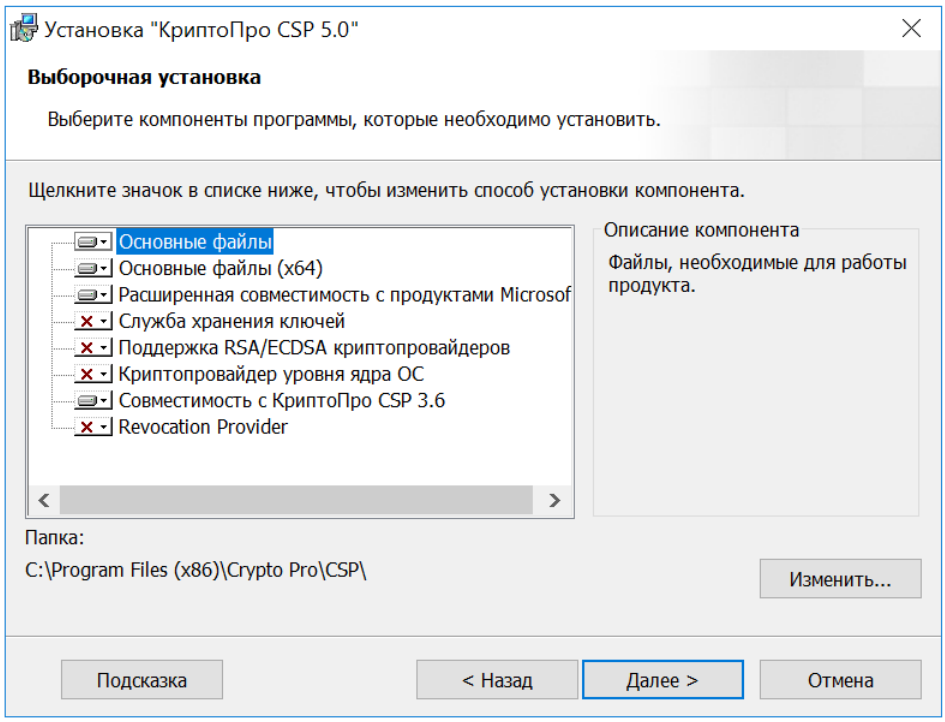


Рисунок 9. Выборочная установка

Для установки доступны следующие компоненты:

- **Расширенная совместимость с продуктами Microsoft** — обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express, Internet Explorer. Необходим для входа в систему по смарт-картам и TLS.
- **Служба хранения ключей** — обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС (только для пассивных хранилищ ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене).
- **Поддержка RSA/ECDSA криптопровайдеров** — обеспечивает взаимодействие с криптопровайдерами, поддерживающими алгоритмы RSA и ECDSA. Не допускается использовать для защиты информации, отличной от тестовых данных.
- **Криптопровайдер уровня ядра ОС** — необходим для работы криптопровайдера в службах и ядре Windows (TLS-сервер, EFS, IPsec).
- **Совместимость с КриптоПро CSP 3.6** — регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.6. Необходим только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.
- **Revocation Provider** — механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (COC, CRL). Кроме этого предоставляет возможность использования COC, выпущенных по правилам, описанным в RFC 3280.

Примечание. В состав КриптоПро CSP SDK входит описание параметров командной строки установщика Windows `\CHM\msi-readme.txt`, которые удобно использовать для автоматического развертывания дистрибутива.

После нажатия на кнопку **Далее** Мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей (см. Рисунок 10).

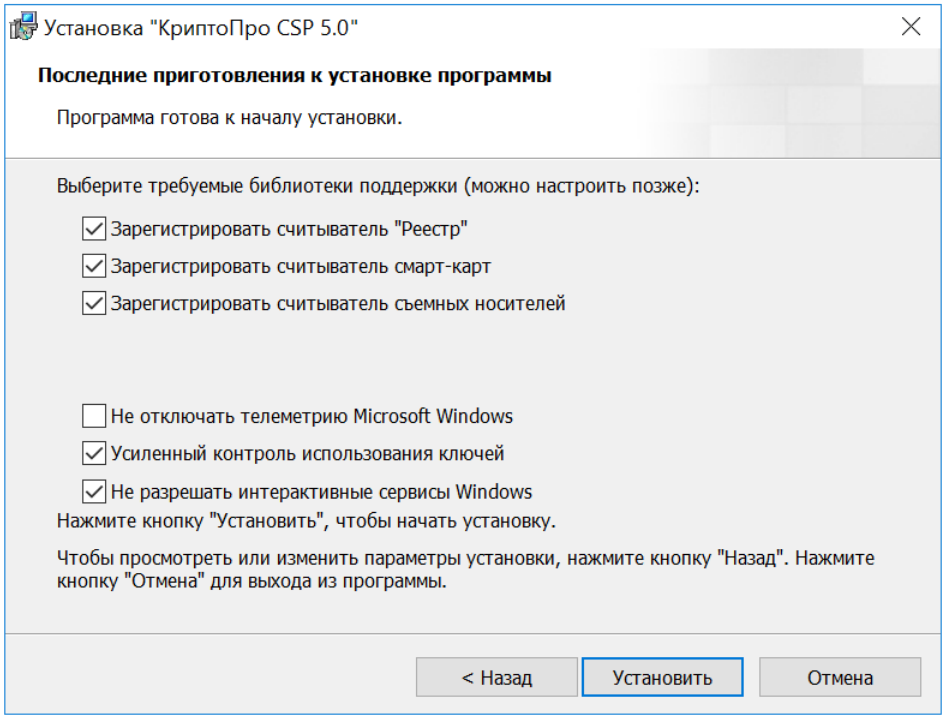


Рисунок 10. Выбор библиотек поддержки, установка усиленного контроля использования ключей и управление сервисами Windows

В окне возможно установить некоторые параметры ОС Windows — службы телеметрии и интерактивных сервисов. По умолчанию при установке СКЗИ на ОС Windows происходит остановка служб телеметрии.

Примечание. Отключение функций телеметрии является обязательным условием эксплуатации СКЗИ под управлением ОС Windows 10/Server 2016.

Также необходимо включить режим усиленного контроля использования ключей. Данный режим осуществляет контроль срока действия долговременных ключей электронной подписи и ключевого обмена, контроль доверенности ключей проверки электронной подписи и контроль корректного использования программного датчика случайных чисел. Использование СКЗИ КриптоПро CSP без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

При выборе усиленного контроля использования ключей появится окно предупреждения с перечнем необходимых действий для корректной настройки криптопровайдера (см. Рисунок 11).

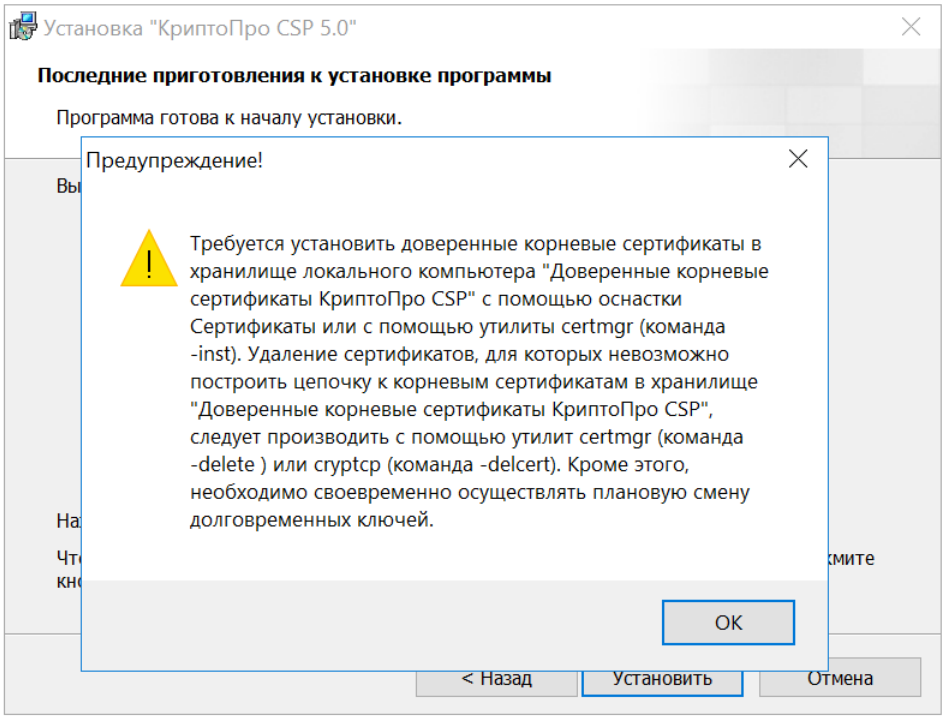


Рисунок 11. Установка усиленного контроля использования ключей

Для начала установки СКЗИ КриптоПро CSP нажмите кнопку **Установить**. В окне Мастера установки будет отображено текущее состояние процесса установки (см. Рисунок 12).

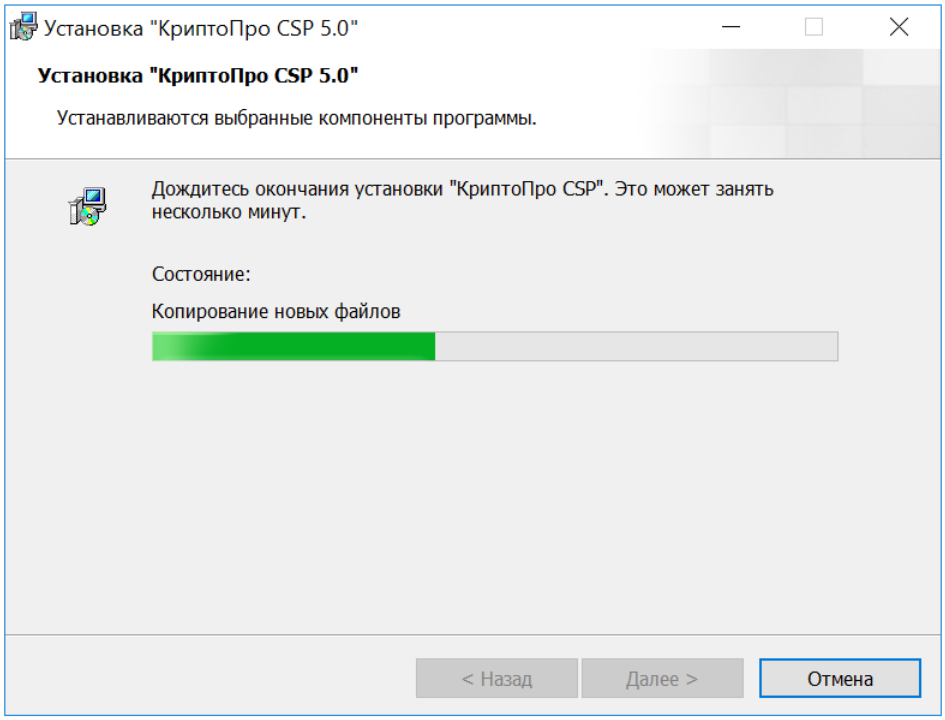


Рисунок 12. Процесс установки КриптоПро CSP

При установке криптопровайдера с включенным режимом усиленного контроля использования ключей будут запрошены данные с ДСЧ. В случае ошибки получения данных будет отображено окно ошибки (см. Рисунок 13).

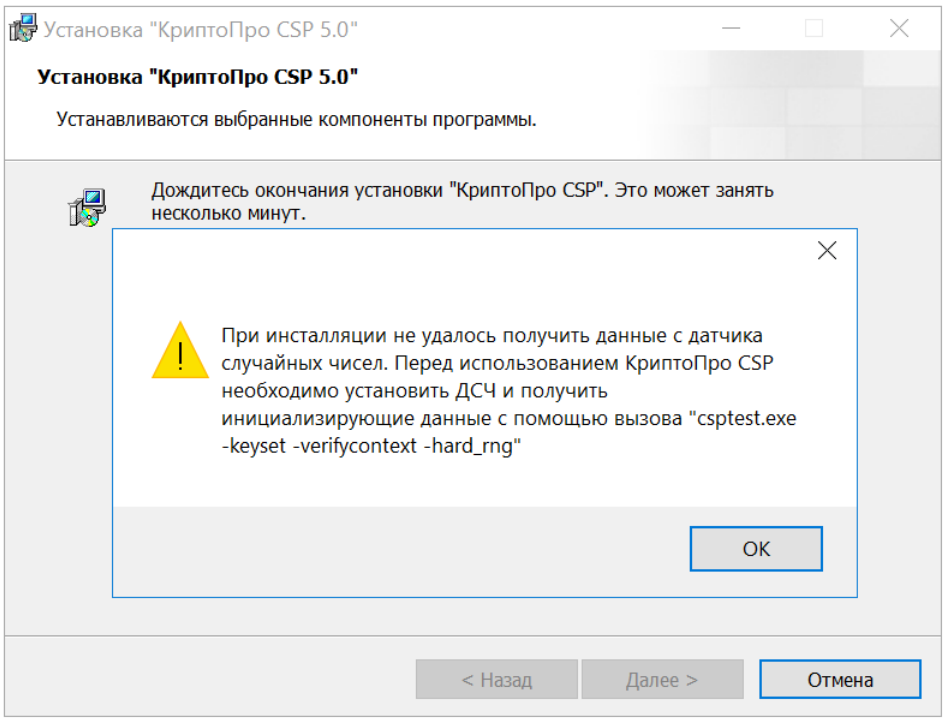


Рисунок 13. Окно ошибки получения данных с ДСЧ

В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, биологический ДСЧ, внешняя гамма или аппаратный ДСЧ).

После завершения установки СКЗИ с включенным режимом усиленного контроля использования ключей **необходимо в обязательном порядке** установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера «CryptoProTrustedStore» («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки **Сертификаты** либо с помощью утилиты `certmgr.exe`:

```
certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file <имя файла сертификата>
```

При завершении установки всех компонентов криптопровайдера Мастер сообщит об успешной установке КриптоПро CSP (см. Рисунок 14). Нажмите кнопку **Готово** для выхода из программы установки.

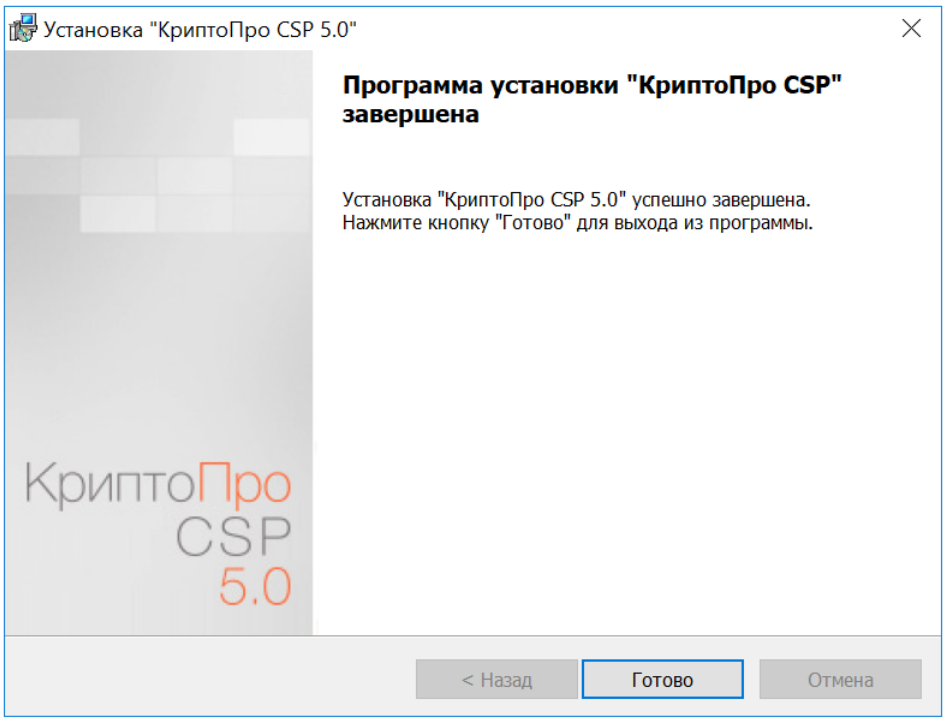


Рисунок 14. Завершение установки КриптоПро CSP

Если программой установки будет предложена перезагрузка компьютера (см. Рисунок 15), нажмите кнопку **Да** для завершения установки и применения изменений криптопровайдера.

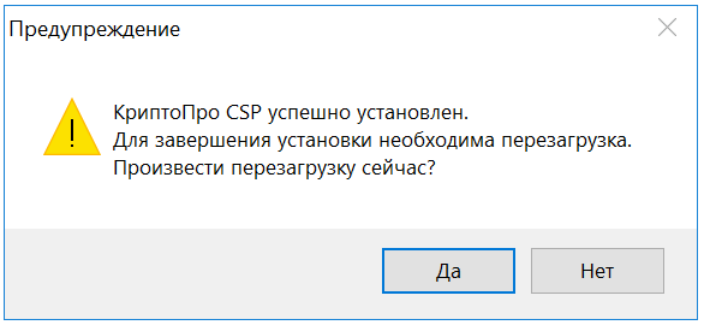


Рисунок 15. Перезагрузка компьютера после установки

2 Интерфейс СКЗИ КриптоПро CSP

2.1 Доступ к панели управления СКЗИ

Контрольная Панель управления СКЗИ КриптоПро CSP доступна как отдельный пункт в группе программ «КРИПТО-ПРО» (меню **Пуск** ⇒ **КРИПТО-ПРО** ⇒ **КриптоПро CSP**) (см. Рисунок 16).

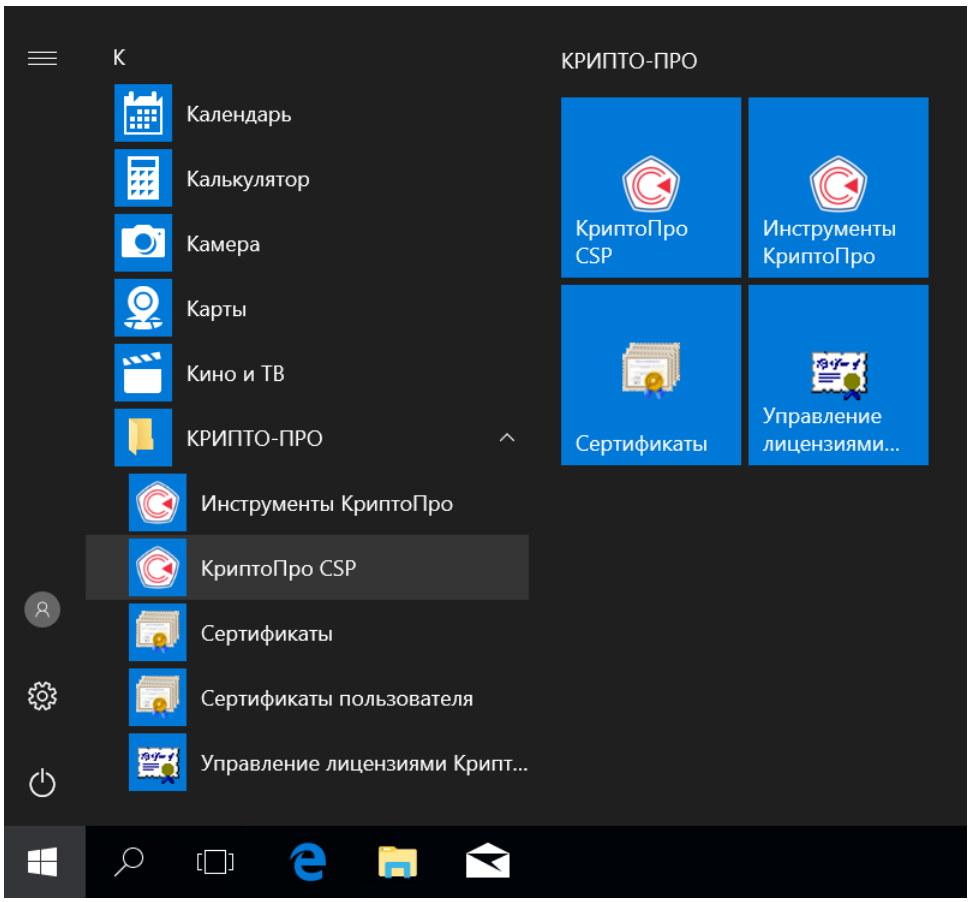


Рисунок 16. Доступ к панели управления КриптоПро CSP

Некоторые функции панели управления КриптоПро CSP также доступны в категории **Система и безопасность** Панели управления ОС Windows (см. Рисунок 17).

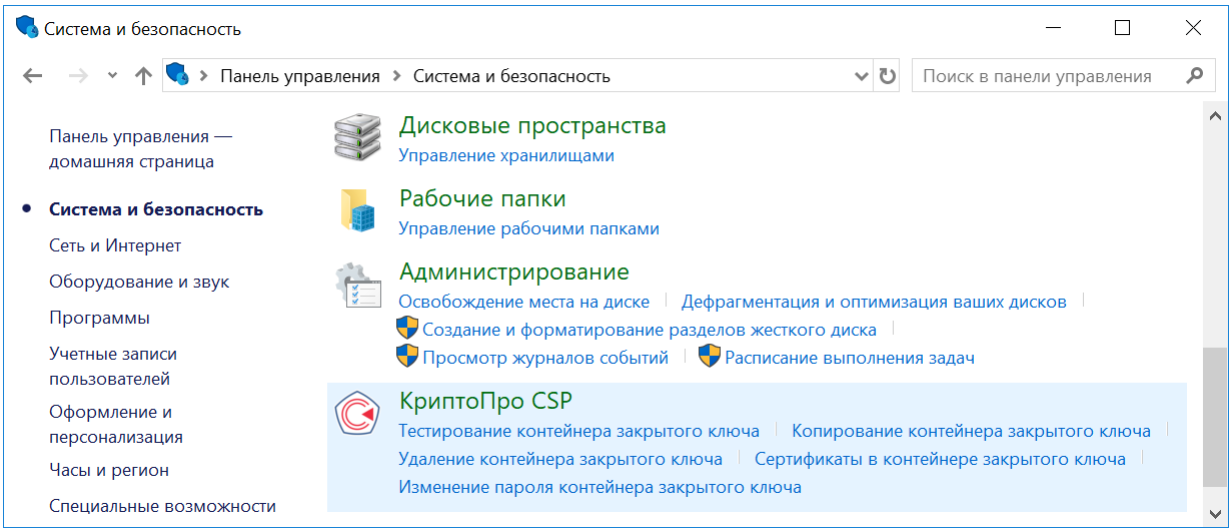


Рисунок 17. Доступ к КриптоПро CSP через панель управления Windows

Панель управления СКЗИ КриптоПро CSP (см. Рисунок 18) осуществляет доступ к настройке функций с помощью вкладок:

- Общие;
- Оборудование;
- Сервис;
- Алгоритмы;
- Безопасность;
- Winlogon;
- Настройки TLS;
- Криптопровайдеры;
- Дополнительно.

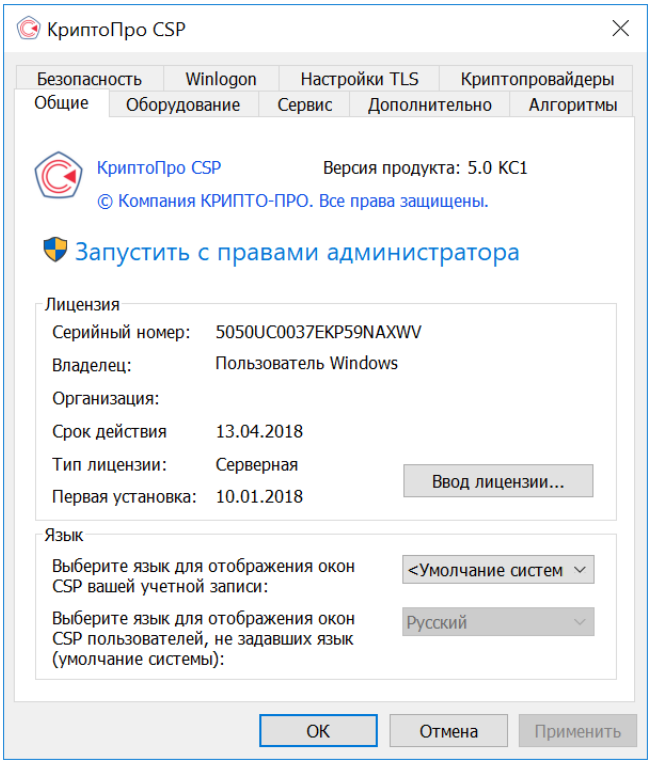


Рисунок 18. Панель управления КриптоПро CSP

2.2 Общие параметры СКЗИ

Вкладка **Общие** панели управления СКЗИ КриптоПро CSP предназначена для просмотра информации о версии установленного ПО СКЗИ КриптоПро CSP, информации о лицензии и ввода нового серийного номера (подробнее см. Ввод серийного номера лицензии), изменения языка работы пользователя с данным ПО.

2.3 Ввод серийного номера лицензии

При установке программного обеспечения КриптоПро CSP пользователю предлагается ввести данные лицензии. Без ввода лицензии пользователю предоставляется ознакомительная лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока нужно ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта. Если КриптоПро CSP используется на клиентской машине, то требуется лицензия клиентского типа, если на сервере — то серверная лицензия.

Для ввода лицензии после установки КриптоПро CSP воспользуйтесь кнопкой **Ввод лицензии** на вкладке **Общие** панели управления КриптоПро CSP. Откроется окно «Сведения о пользователе» (см. Рисунок 20).

Также можно ввести лицензию с помощью утилиты Управление лицензиями КриптоПро PKI. Для этого выполните **Пуск** ⇒ **КРИПТО-ПРО** ⇒ **Управление лицензиями КриптоПро PKI**. В оснастке **Управление лицензиями КриптоПро PKI** выберите продукт, лицензию на который Вы хотите ввести. В контекстном меню выберите **Все задачи** ⇒ **Ввести серийный номер** (см. Рисунок 19).

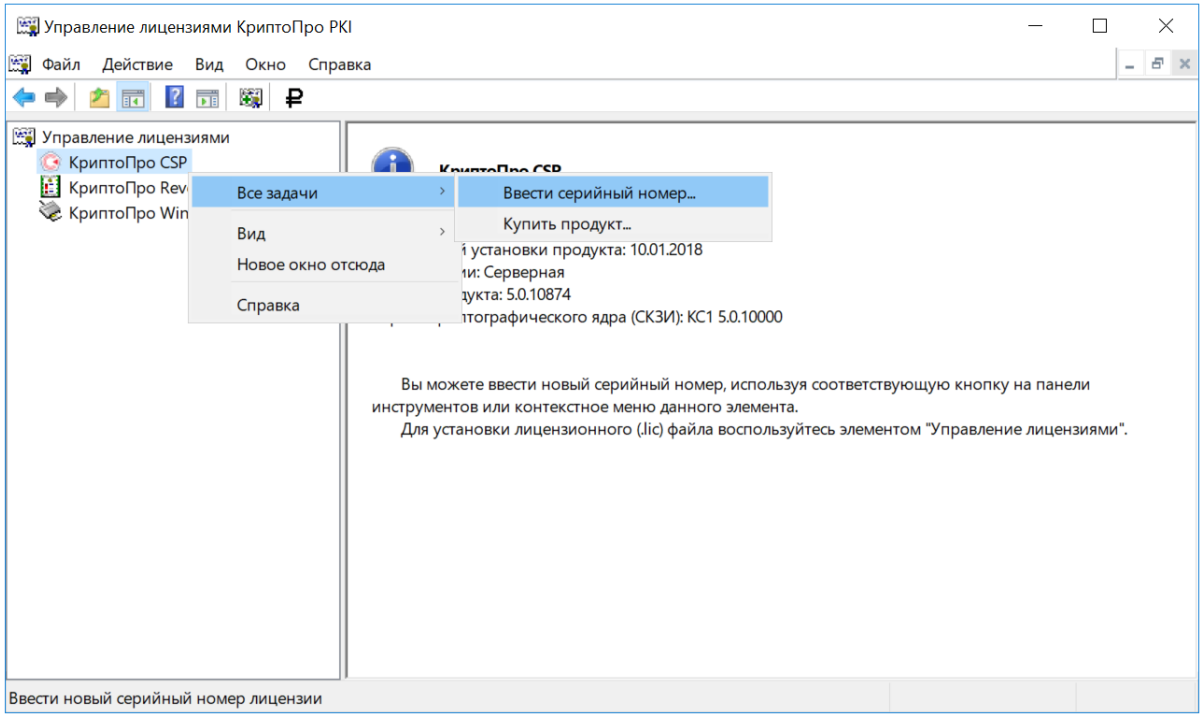


Рисунок 19. Ввод серийного номера

Откроется окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести 25-значный серийный номер с бланка Лицензии в соответствующие поля ввода (см. Рисунок 20).

После ввода и нажатия клавиши **OK** данные о лицензии сохранятся или обновятся.

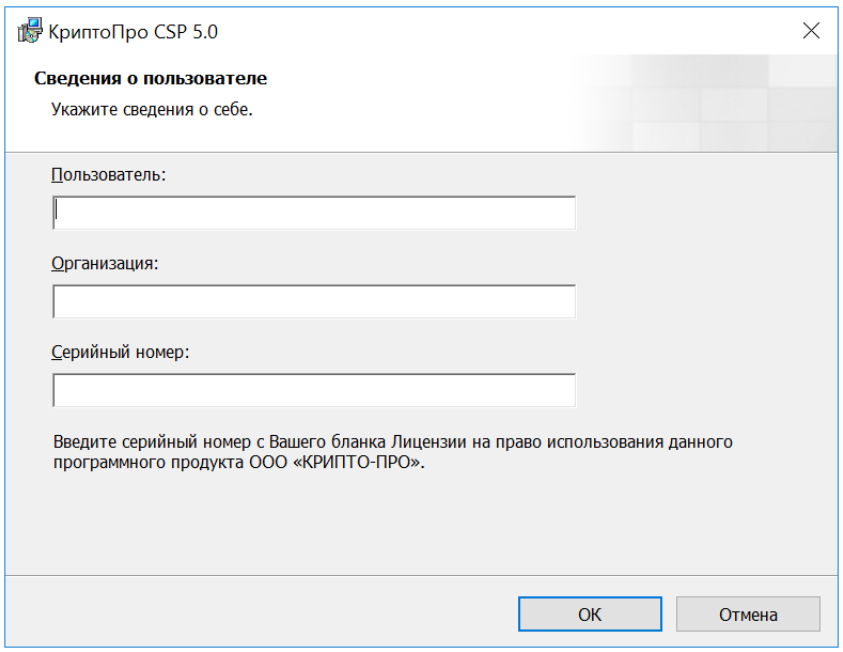


Рисунок 20. Ввод данных лицензии

2.4 Настройка оборудования СКЗИ

Вкладка **Оборудование** панели управления СКЗИ предназначена для изменения набора устройств хранения и считывания ключевой информации и ДСЧ.

По умолчанию поддерживаются все считыватели смарт-карт (и соответствующие им типы носителей), все дисководы съёмных дисков, в том числе USB-флэш-накопители.

Для уровня защиты КС1 считыватель «Реестр» выбирается по умолчанию при установке (см. Рисунок 10).

В исполнении СКЗИ по уровню защиты КС1 предустановлен Биологический ДСЧ.

2.4.1 Управление считывателями ключевой информации

2.4.1.1 Добавление считывателя

Для добавления считывателя откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели**.

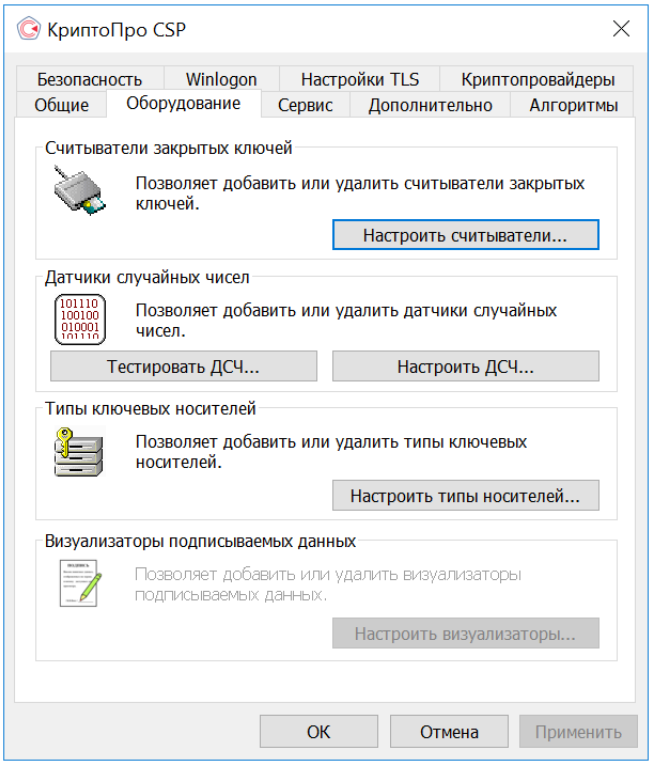


Рисунок 21. Вкладка **Оборудование** панели управления

При нажатии на кнопку **Настроить считыватели** откроется окно «Управление считывателями» (см. Рисунок 22).

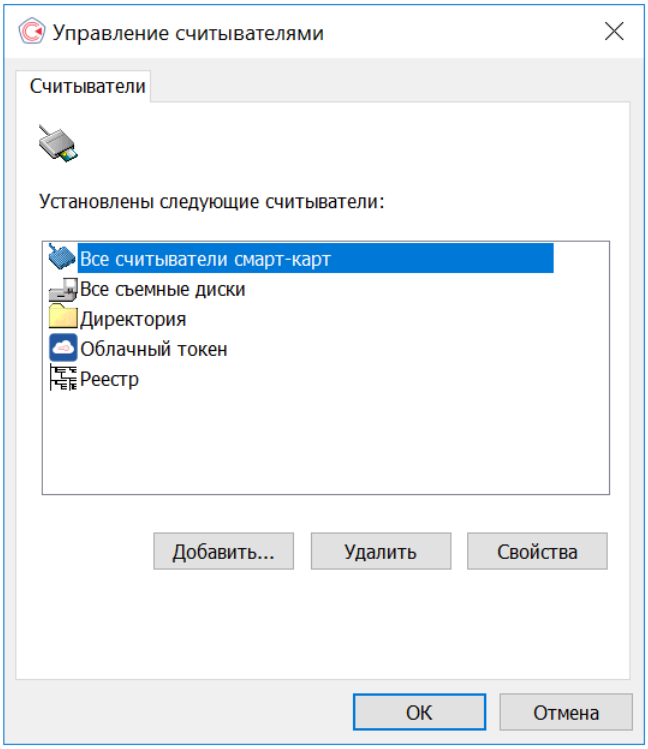


Рисунок 22. Управление считывателями

Для того чтобы в КриптоПро CSP стало доступным использование нового считывателя, нажмите кнопку **Добавить**. Запустится Мастер установки считывателя (см. Рисунок 23).

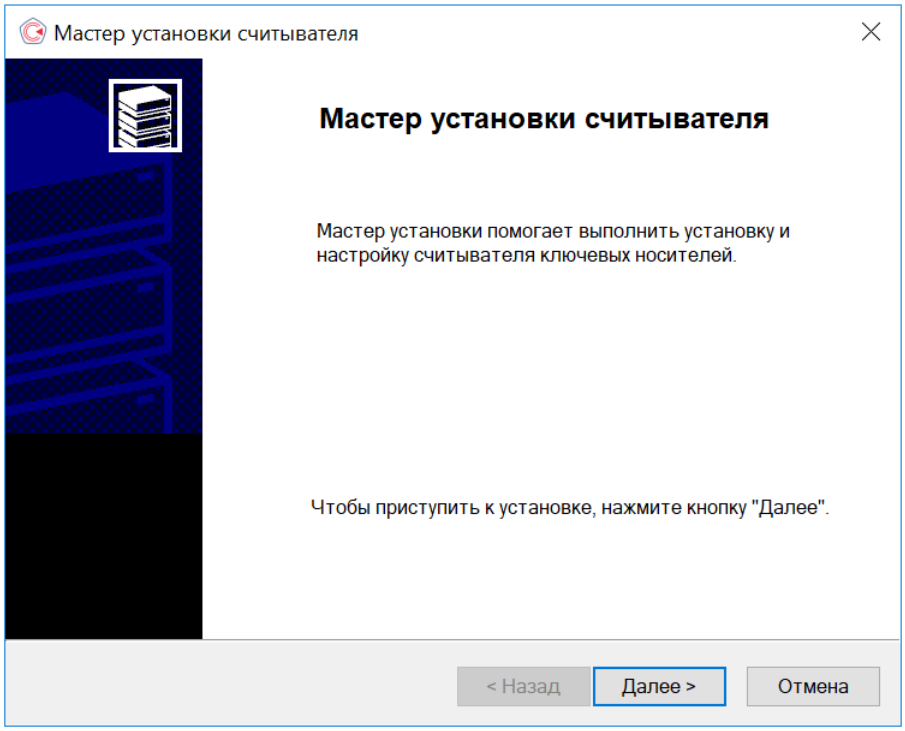


Рисунок 23. Запуск Мастера установки считывателя

Нажмите кнопку **Далее**, чтобы перейти к шагу «Выбор считывателя» (см. Рисунок 24). Выберите из списка считыватель, который следует добавить.

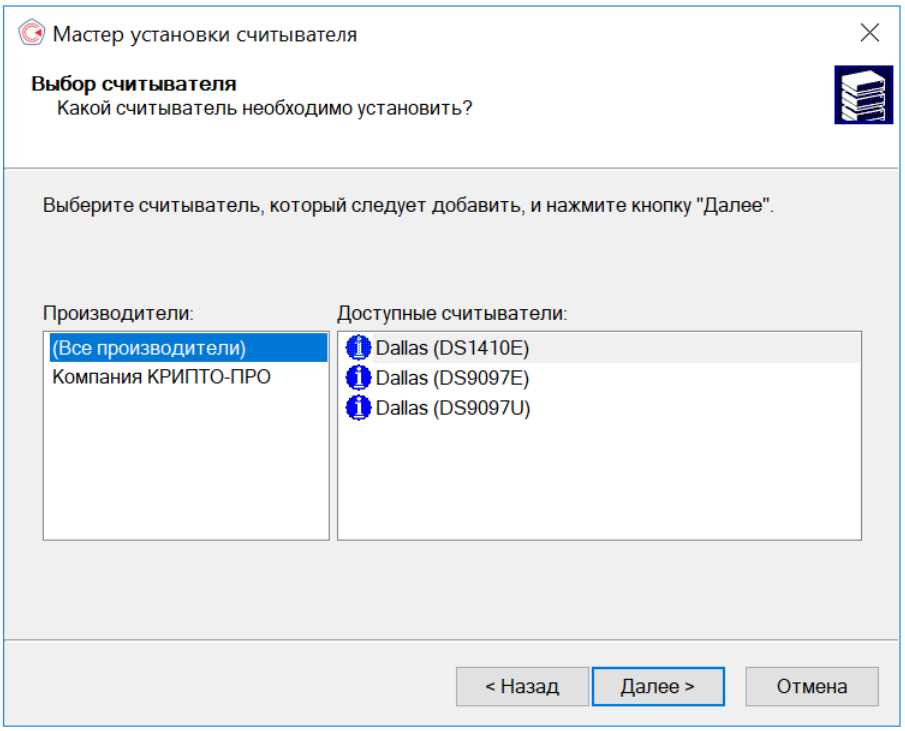


Рисунок 24. Выбор считывателя

В зависимости от выбранного считывателя может потребоваться выбор соединения для этого устройства. В таком случае на следующем шаге мастера выводится окно «Выбор соединения» (см. Рисунок 25). В этом окне выберите

соединение для считывателя и нажмите кнопку **Далее**.

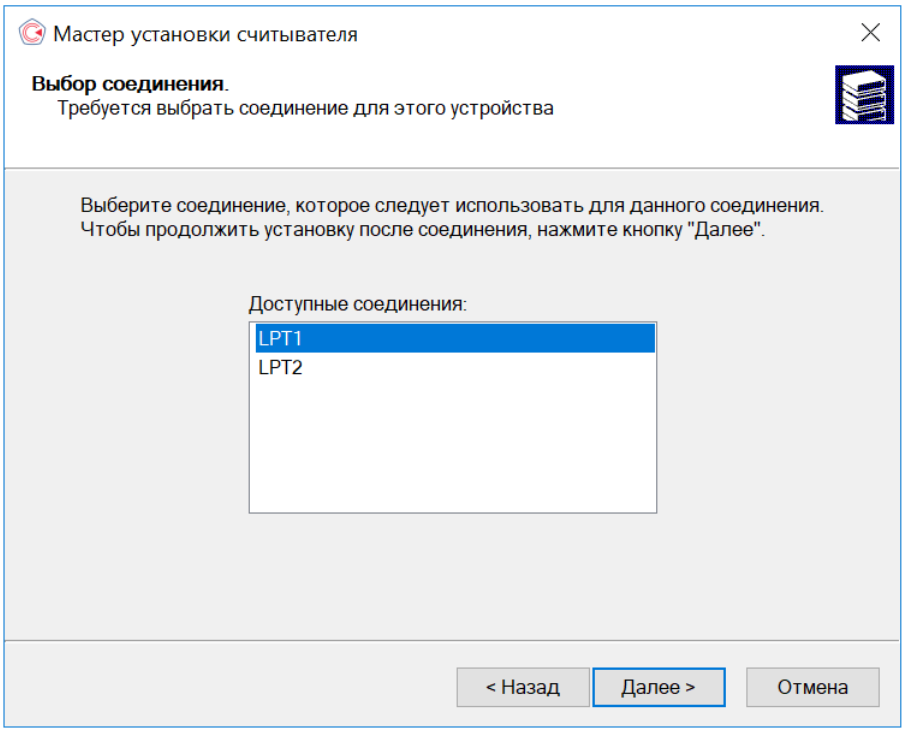


Рисунок 25. Выбор соединения для считывателя

На следующем шаге выводится окно «Имя считывателя» (см. Рисунок 26). В этом окне введите имя выбранного считывателя и нажмите кнопку **Далее**.

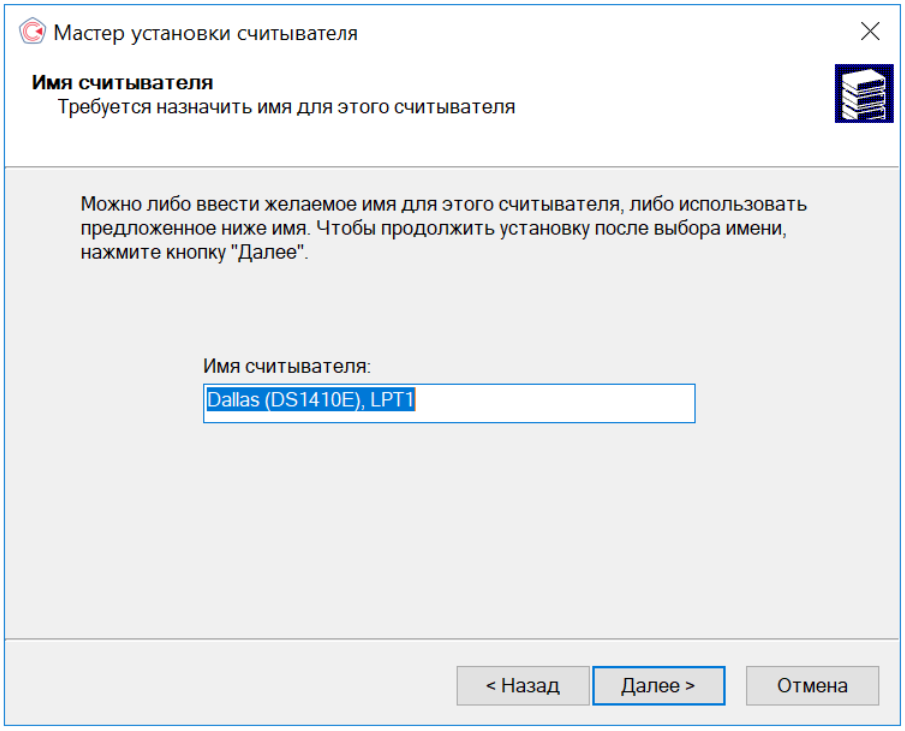


Рисунок 26. Имя считывателя

Последний шаг — окно «Завершение работы мастера установки считывателя» (см. Рисунок 27). Внимательно

прочитайте текст в этом окне, нажмите кнопку **Готово** и перезагрузите компьютер.

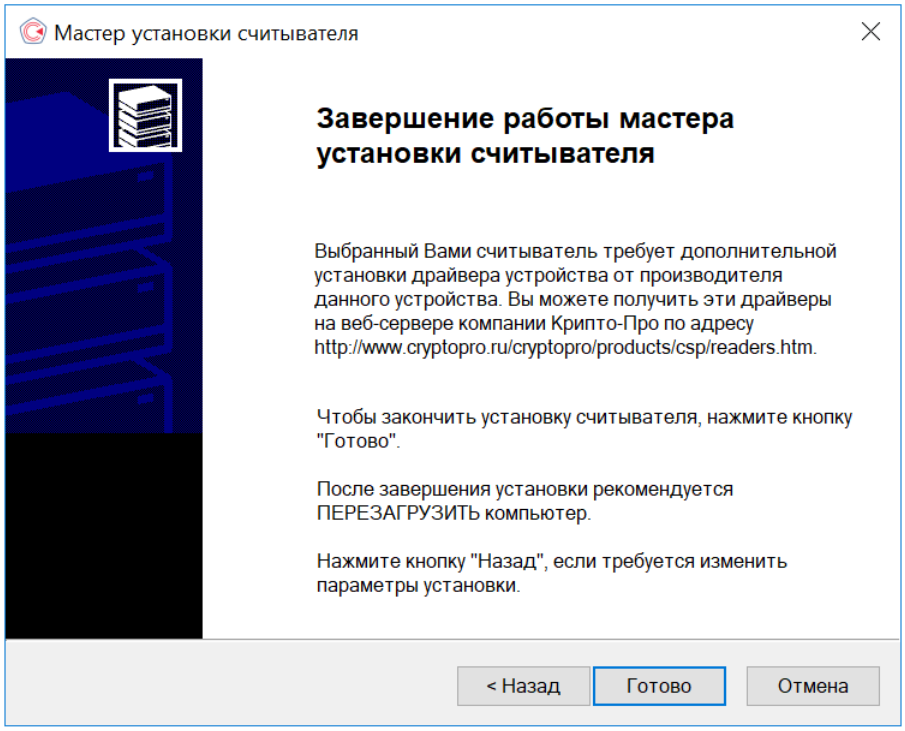


Рисунок 27. Завершение работы мастера установки считывателя

Примечание. Имеется возможность установки драйверов сторонних производителей, обеспечивающих взаимодействие КриптоПро CSP с аппаратной частью в случае, если они не входят в состав дистрибутива СКЗИ. Для их установки следует воспользоваться программой установки, поставляемой производителями таких устройств. Например, если КриптоПро CSP уже установлен, и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

2.4.1.2 Удаление считывателя

Для удаления считывателя откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели**.

При нажатии на кнопку **Настроить считыватели** откроется окно «Управление считывателями» (см. Рисунок 28). Выберите считыватель, который требуется сделать недоступным, и нажмите кнопку **Удалить**. В открывшемся диалоге подтвердите удаление считывателя, нажав кнопку **OK** (см. Рисунок 29). После подтверждения действия считыватель станет недоступен для использования в работе криптопровайдера.

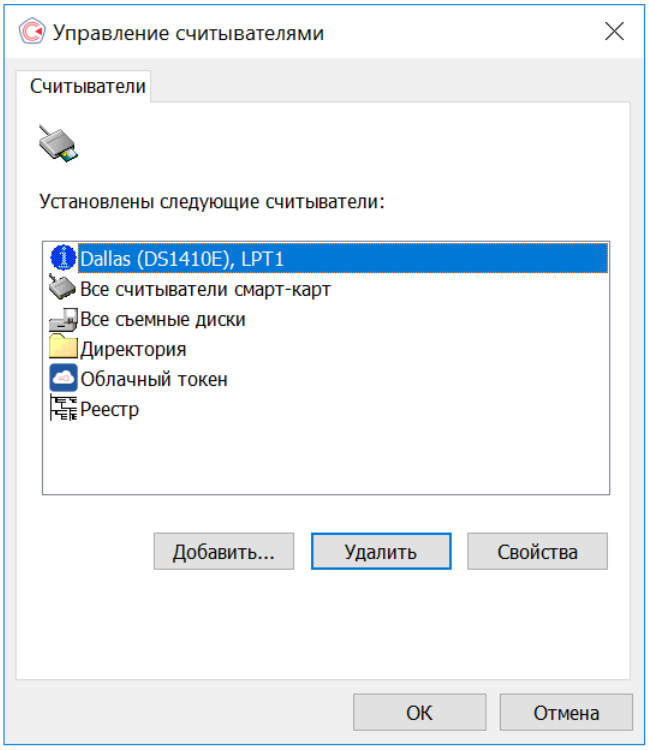


Рисунок 28. Выбор считывателя для удаления

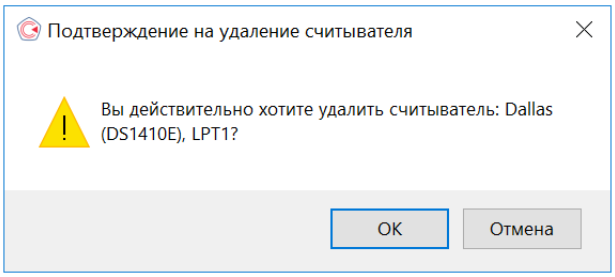


Рисунок 29. Подтверждение на удаление считывателя

2.4.1.3 Просмотр свойств считывателя

Для просмотра свойств считывателя откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP нажмите кнопку **Настроить считыватели**.

При нажатии на кнопку **Настроить считыватели** откроется окно «Управление считывателями» (см. Рисунок 22). Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**. Откроется окно со справочной информацией о выбранном считывателе, в том числе, данными о состоянии устройства (см. Рисунок 30). После просмотра свойств считывателя нажмите кнопку **OK**.

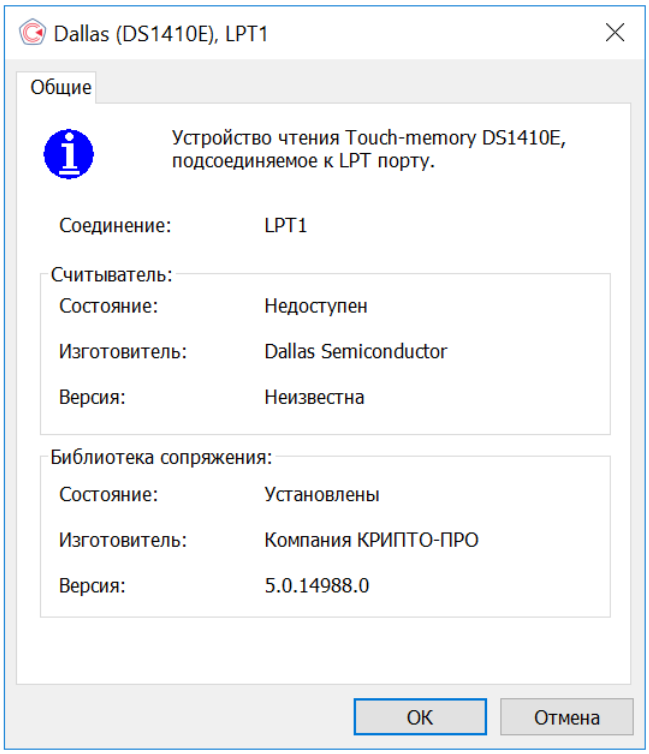


Рисунок 30. Свойства считывателя

2.4.2 Управление носителями ключевой информации

2.4.2.1 Добавление носителя

Для добавления носителя ключевой информации откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей**.

При нажатии на кнопку **Настроить типы носителей** откроется окно «Управление ключевыми носителями» (см. Рисунок 31).

Примечание. Носители Магистра, Магистра Сбербанк/BGS, Оскар, Оскар CSP 2.0, РИК являются смарткартами. Носители типа Rutoken и eToken являются USB ключами.

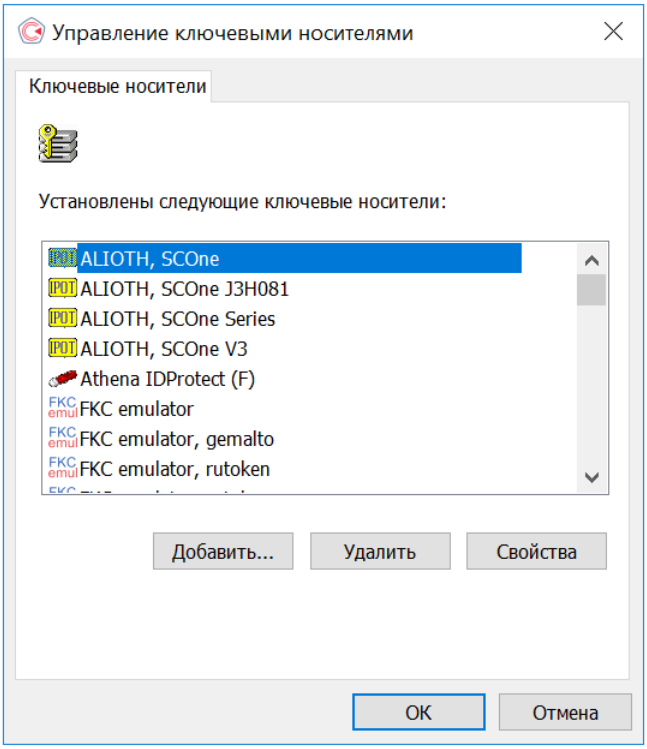


Рисунок 31. Управление ключевыми носителями

Для того чтобы в КриптоПро CSP стало доступным использование ключевого носителя, нажмите кнопку **Добавить**. Запустится мастер установки ключевого носителя (см. Рисунок 32).

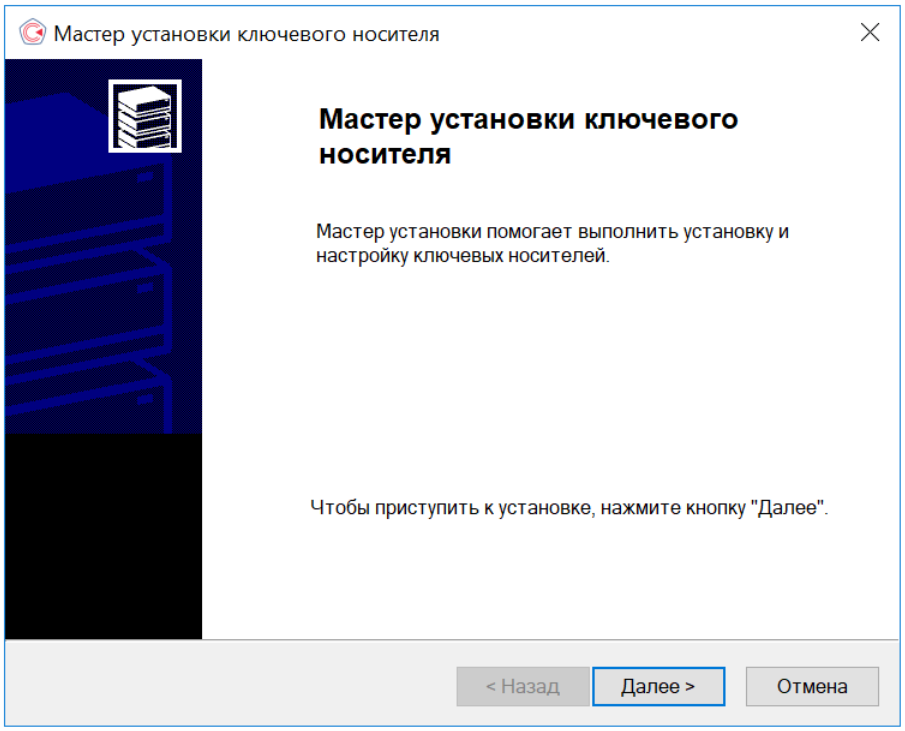


Рисунок 32. Запуск мастера установки ключевого носителя

Нажмите кнопку **Далее**, чтобы перейти к шагу выбора ключевого носителя (см. Рисунок 33). Выберите ключевой носитель, который следует сделать доступным, и нажмите кнопку **Далее**.

Примечание. Запрещается использовать несъёмные носители, а также носители, для которых не обеспечивается непрерывный контроль.

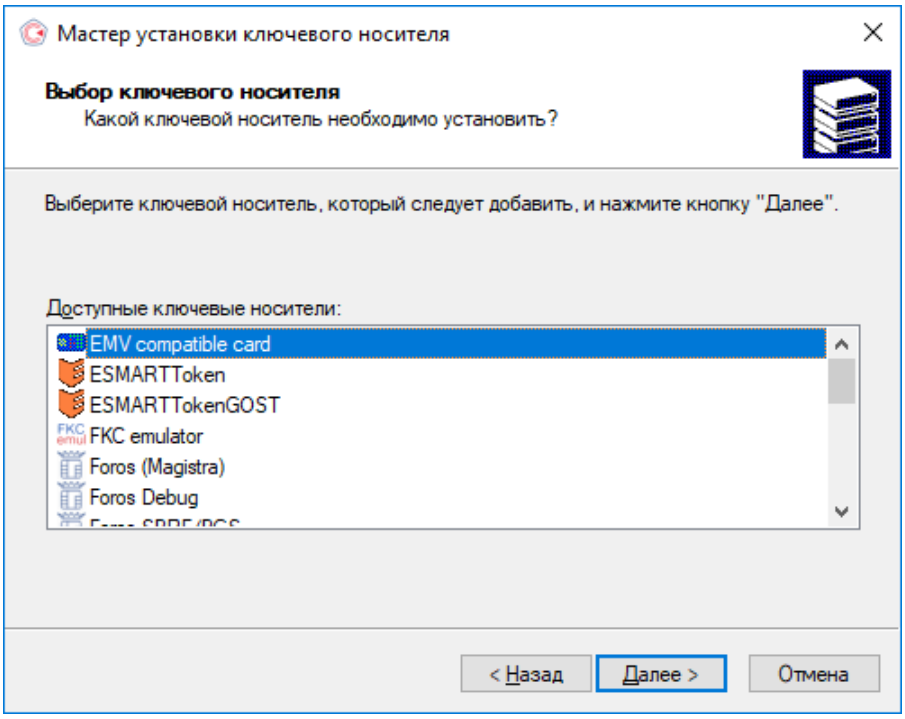


Рисунок 33. Выбор ключевого носителя

После выбора ключевого носителя откроется окно «Имя ключевого носителя» (см. Рисунок 34). В этом окне введите имя выбранного носителя и нажмите кнопку **Далее**.

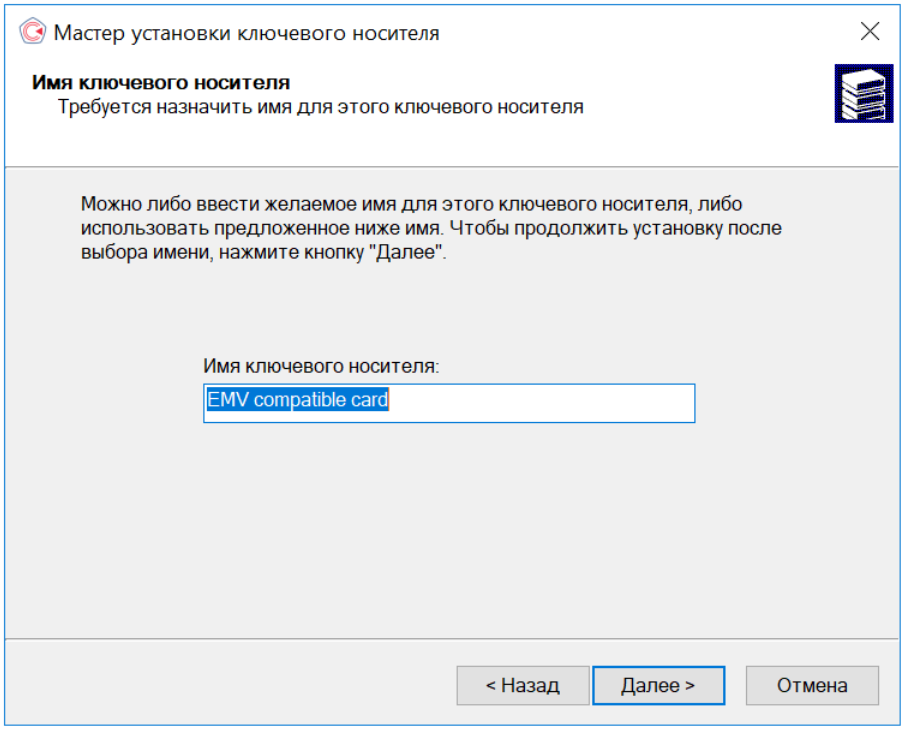


Рисунок 34. Имя ключевого носителя

В зависимости от типа ключевого носителя следующие шаги мастера могут различаться. Например, для EMV карт будет отображено окно «Разметка карты» (см. Рисунок 35). В этом окне нужно указать разметку карты, после чего перейти к следующему шагу, нажав кнопку **Далее**.

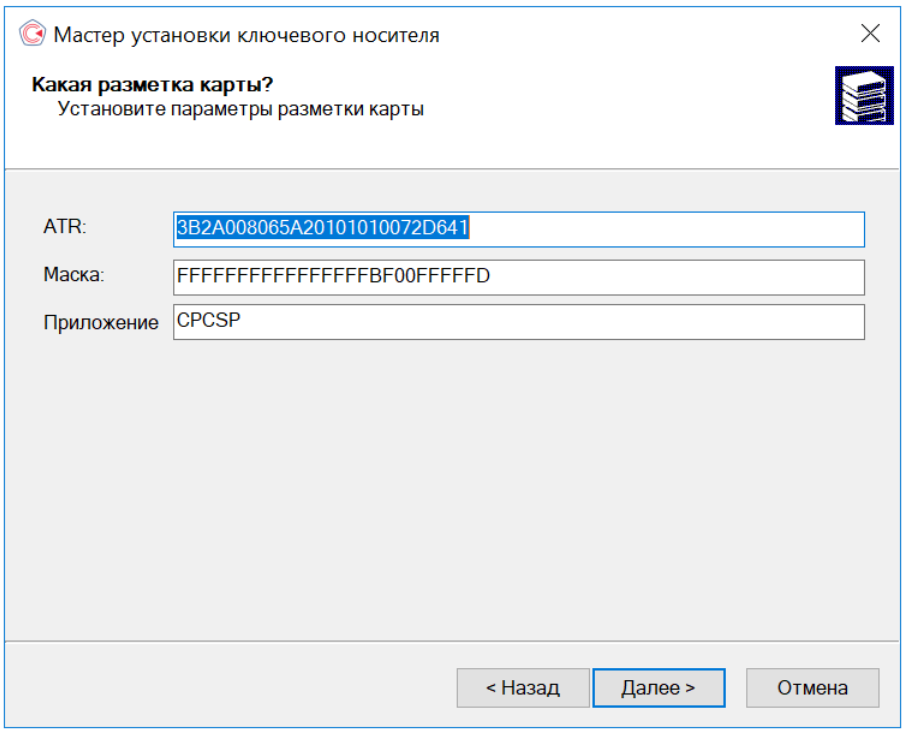


Рисунок 35. Окно «Разметка карты»

Последний шаг — окно «Завершение работы мастера установки ключевого носителя» (см. Рисунок 36). Для завершения установки ключевого носителя нажмите кнопку **Готово**. Установленный ключевой носитель отобразится в списке окна «Управление ключевыми носителями» (см. Рисунок 31).

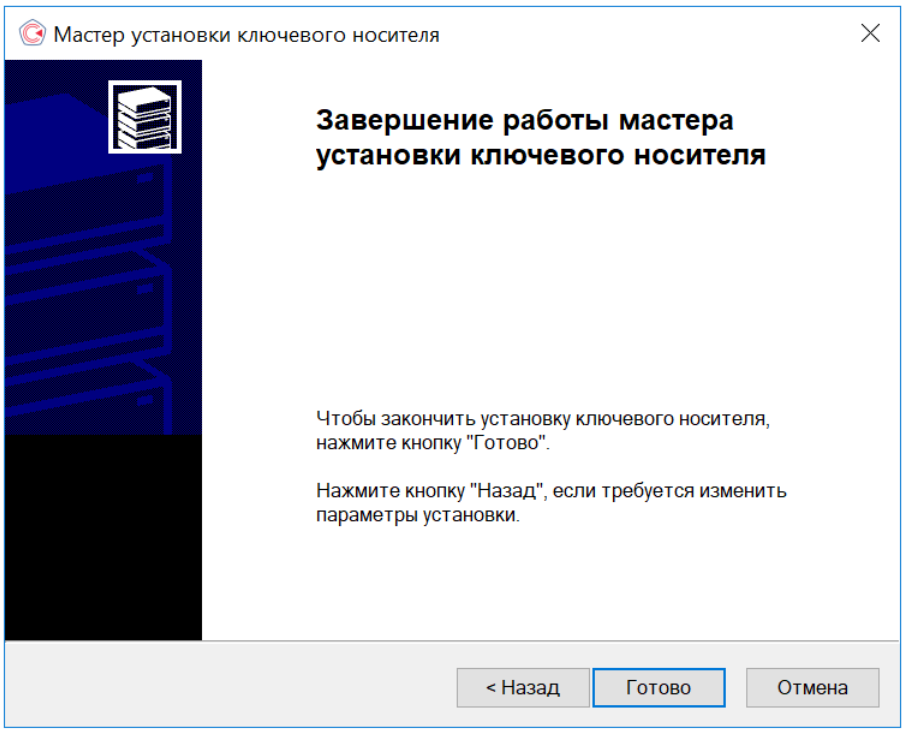


Рисунок 36. Завершение работы мастера установки ключевого носителя

2.4.2.2 Удаление ключевого носителя

Для удаления ключевого носителя откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей**.

При нажатии на кнопку **Настроить типы носителей** откроется окно «Управление ключевыми носителями» (см. Рисунок 37). Выберите ключевой носитель, который требуется сделать недоступным, и нажмите кнопку **Удалить**. В открывшемся диалоге подтвердите удаление ключевого носителя, нажав кнопку **OK** (см. Рисунок 38). После подтверждения действия ключевой носитель станет недоступен для использования в работе криптопровайдера.

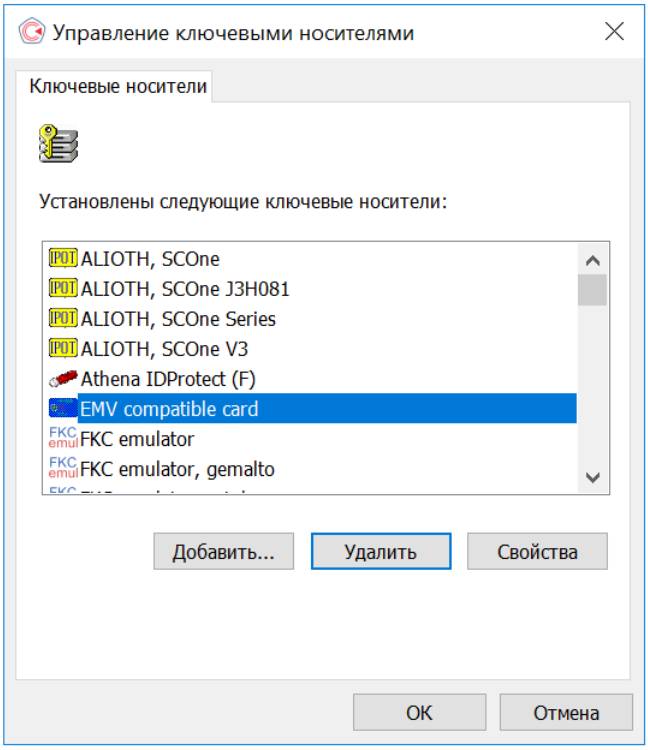


Рисунок 37. Выбор ключевого носителя для удаления

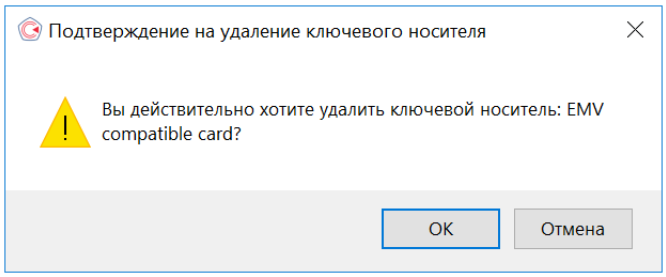


Рисунок 38. Подтверждение на удаление ключевого носителя

2.4.2.3 Просмотр свойств ключевого носителя

Для просмотра свойств ключевого носителя откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP нажмите кнопку **Настроить типы носителей**.

При нажатии на кнопку **Настроить типы носителей** откроется окно «Управление ключевыми носителями» (см. Рисунок 31). Выберите ключевой носитель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**. Откроется окно со справочной информацией о выбранном ключевом носителе (см. Рисунок 39).

Чтобы некоторые ключевые носители были доступны при аутентификации Winlogon (подробнее см. разд. 5), необходимо зарегистрировать их с помощью кнопки **Зарегистрировать в Winlogon**. Для управления регистрацией носителя в Winlogon панель управления должна быть запущена от имени администратора.

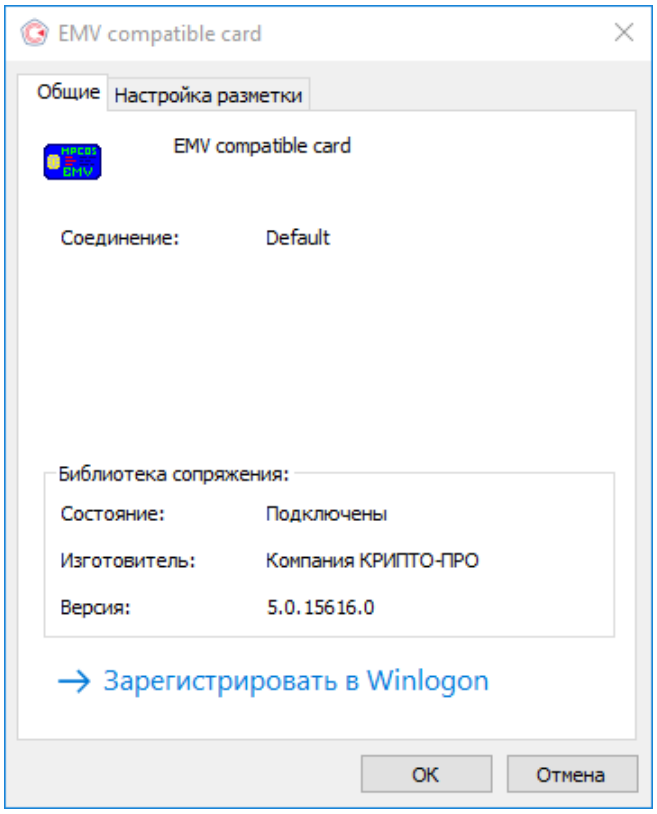


Рисунок 39. Свойства ключевого носителя

2.4.3 Управление датчиками случайных чисел (ДСЧ)

2.4.3.1 Добавление ДСЧ

При настройке ДСЧ и загрузке динамических библиотек должно быть установлено программное обеспечение, соответствующее аппаратному средству. Подключение ДСЧ должно соответствовать установкам программно-аппаратного комплекса.

Для добавления ДСЧ откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

При нажатии на кнопку **Настроить ДСЧ** откроется окно «Управление датчиками случайных чисел» (см. Рисунок 40).

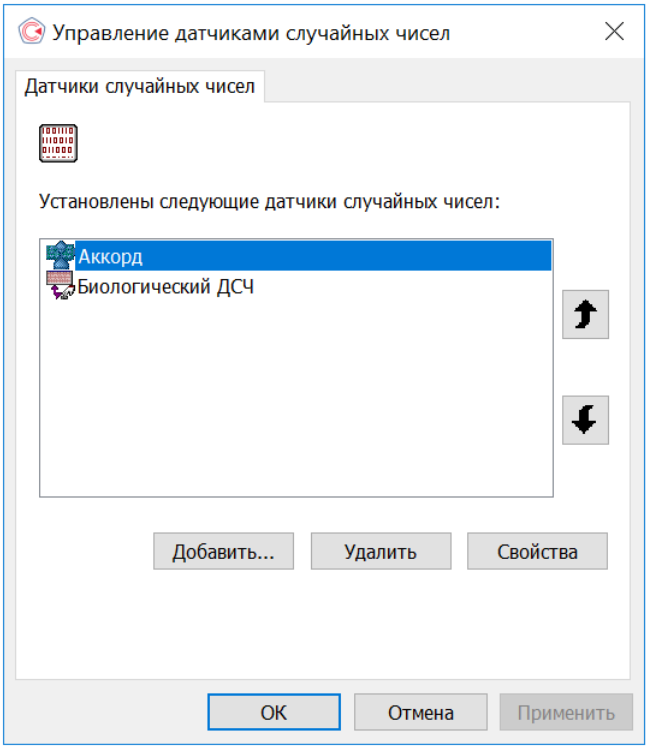


Рисунок 40. Управление датчиками случайных чисел

Для того чтобы в КриптоПро CSP стало доступным использование ДСЧ, нажмите кнопку **Добавить**. Запустится мастер установки ДСЧ (см. Рисунок 41).

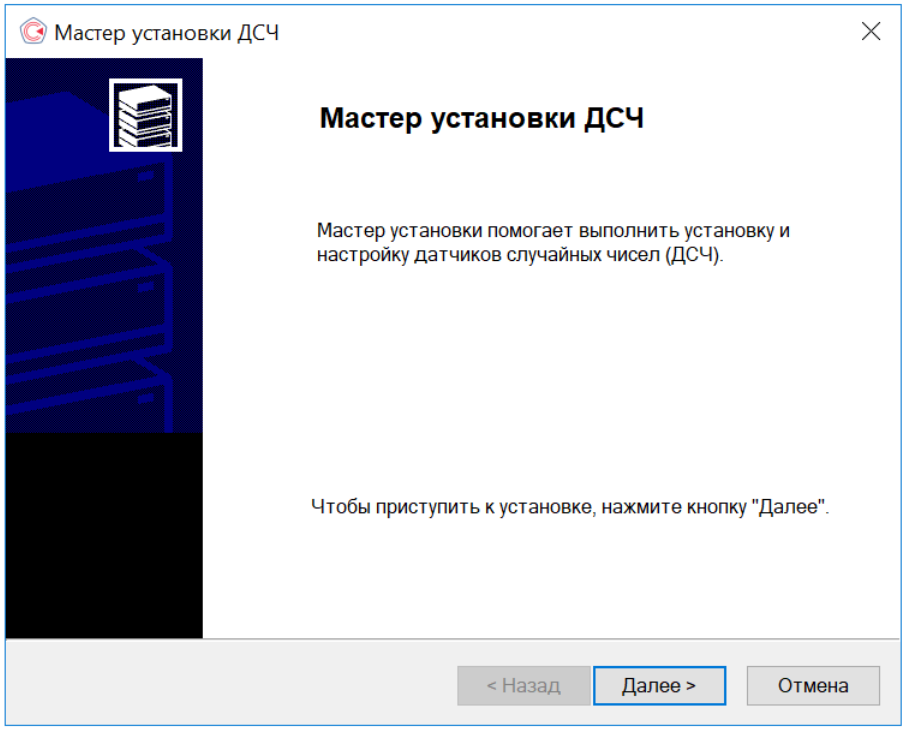


Рисунок 41. Запуск мастера установки ДСЧ

Нажмите кнопку **Далее**, чтобы перейти к шагу выбора ДСЧ (см. Рисунок 42). Выберите ДСЧ, который следует сделать доступным, и нажмите кнопку **Далее**.

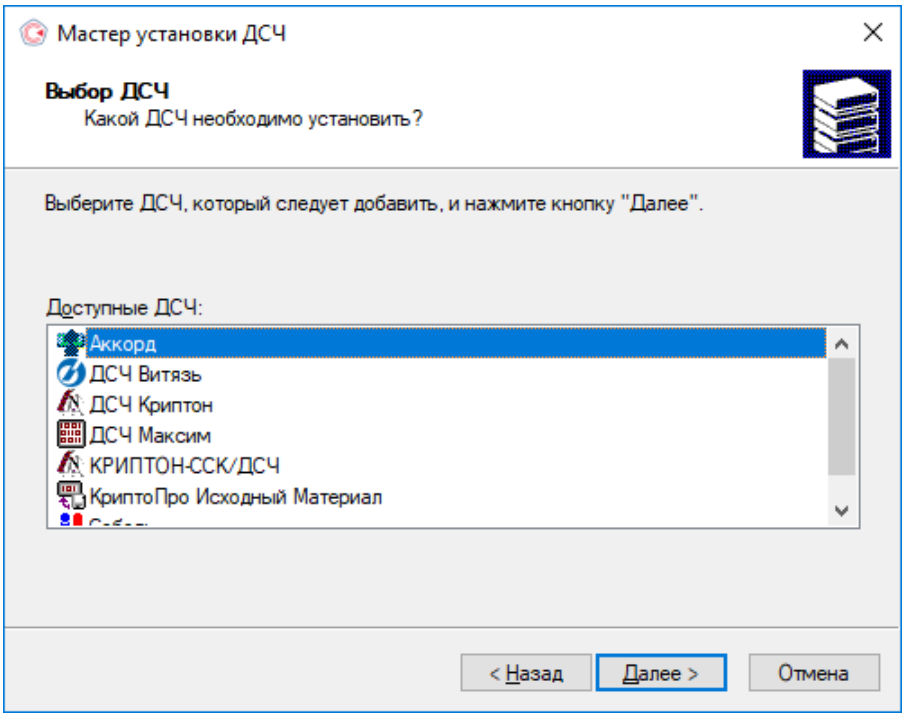


Рисунок 42. Выбор ДСЧ

После выбора ключевого носителя откроется окно «Имя ДСЧ» (см. Рисунок 43). В этом окне введите имя выбранного ДСЧ и нажмите кнопку **Далее**.

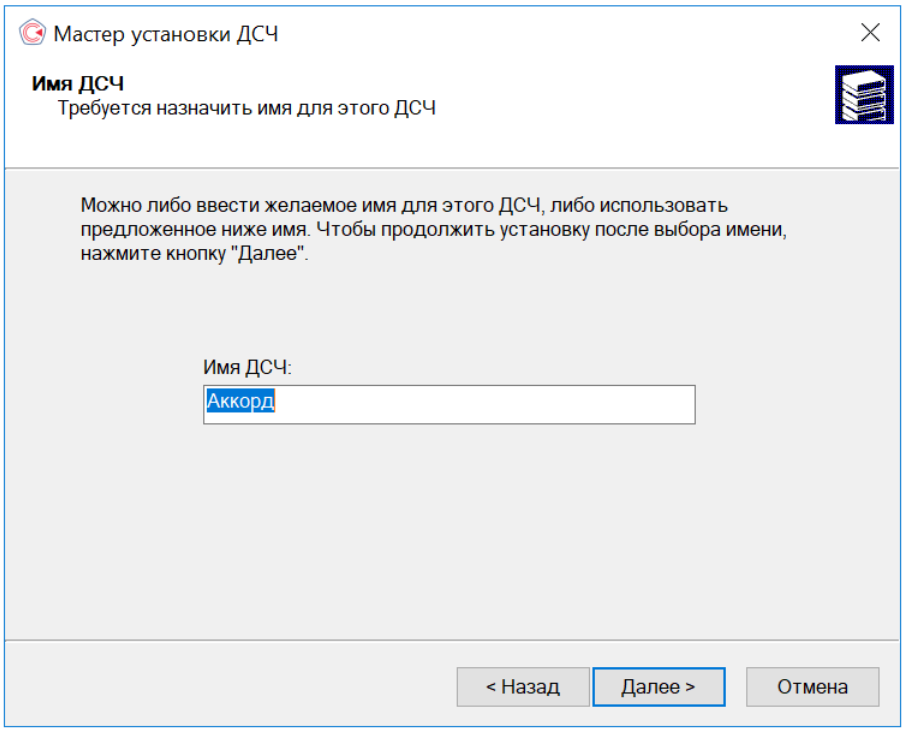


Рисунок 43. Имя ДСЧ

Последний шаг — окно «Завершение работы мастера установки ДСЧ» (см. Рисунок 44). Для завершения установки ДСЧ нажмите кнопку **Готово** и перезагрузите компьютер.

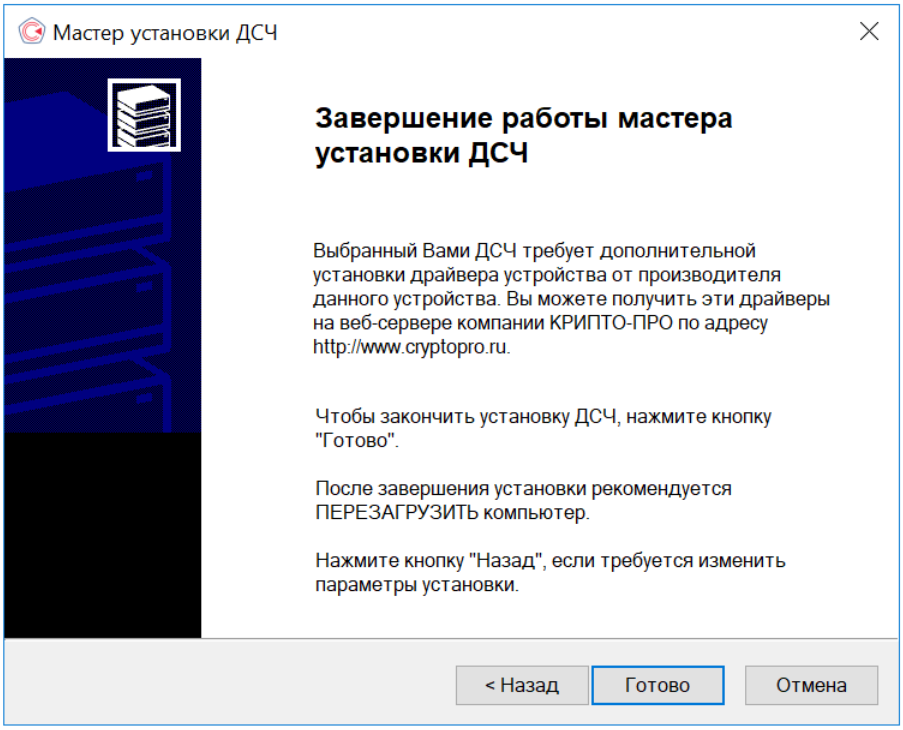


Рисунок 44. Завершение работы мастера установки ДСЧ

2.4.3.2 Удаление ДСЧ

Для удаления ДСЧ откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

При нажатии на кнопку **Настроить ДСЧ** откроется окно «Управление датчиками случайных чисел» (см. Рисунок 45). Выберите ДСЧ, который требуется сделать недоступным, и нажмите кнопку **Удалить**. В открывшемся диалоге подтвердите удаление ДСЧ, нажав кнопку **OK** (см. Рисунок 46). После подтверждения действия ДСЧ станет недоступен для использования в работе криптопровайдера.

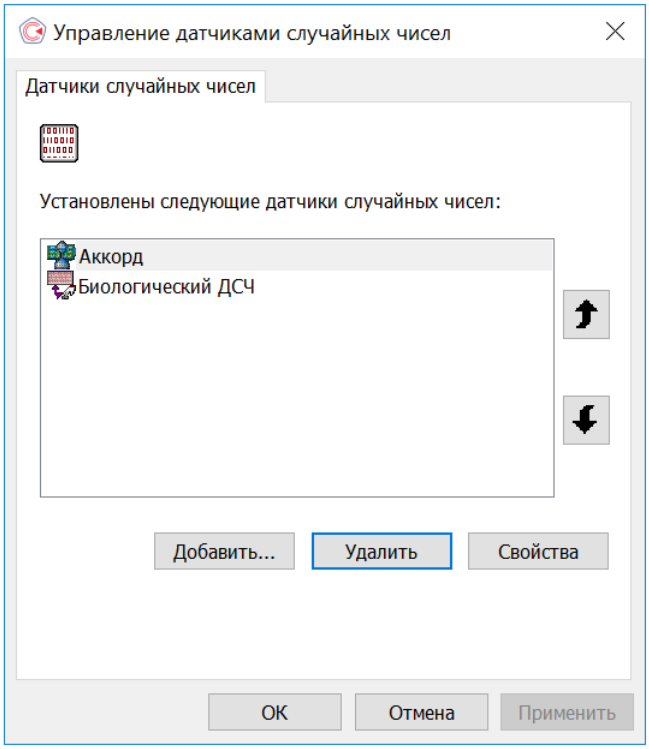


Рисунок 45. Выбор ДСЧ для удаления

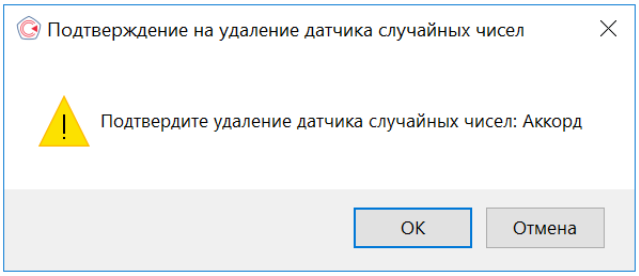


Рисунок 46. Подтверждение на удаление ДСЧ

2.4.3.3 Просмотр свойств ДСЧ

Для просмотра свойств ДСЧ откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP нажмите кнопку **Настроить ДСЧ**.

При нажатии на кнопку **Настроить ДСЧ** откроется окно «Управление датчиками случайных чисел» (см. Рисунок 40). Выберите ДСЧ, свойства которого требуется просмотреть, и нажмите кнопку **Свойства**. Откроется окно со справочной информацией о выбранном ДСЧ, в том числе, данными о состоянии устройства (см. Рисунок 39). После просмотра свойств ключевого носителя нажмите кнопку **OK**.

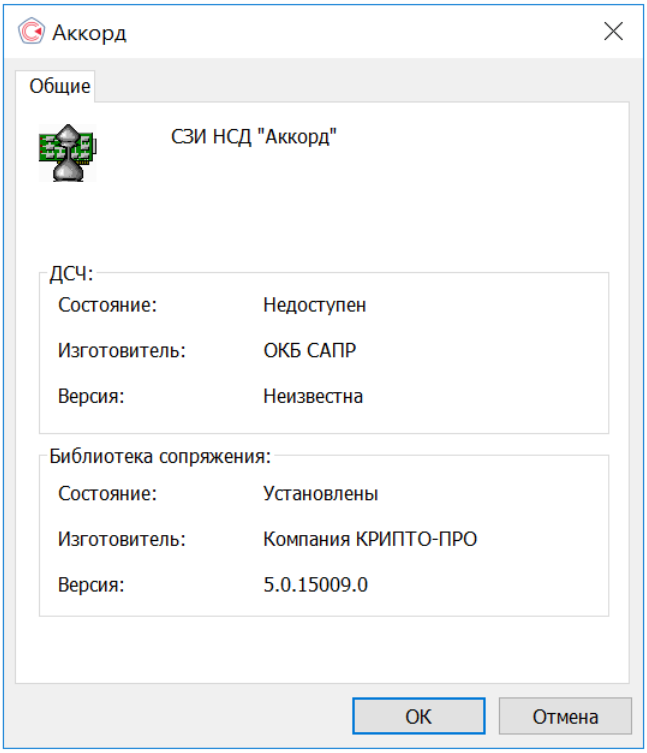


Рисунок 47. Свойства ДСЧ

Примечание. Если в СКЗИ настроено несколько ДСЧ, то при формировании исходной ключевой информации будет использоваться ДСЧ, находящийся в верхней строке списка установленных ДСЧ. Если ДСЧ не установлен, то будет использован следующий и т.д. Например, если установлено два датчика случайных чисел — БиоДСЧ и ДСЧ Электронного замка «Соболь», они находятся в состоянии «подключен» и в верхней строке списка ДСЧ указан ДСЧ Электронного замка «Соболь», то формирование исходной ключевой информации будет осуществляться на ДСЧ Электронного замка «Соболь».

Для использования БиоДСЧ необходимо с помощью кнопок  и  переместить его на верхнюю позицию в списке.

2.4.3.4 Тестирования ДСЧ

Для проверки работоспособности установленных ДСЧ откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP нажмите кнопку **Тестировать ДСЧ**.

При нажатии на кнопку **Тестировать ДСЧ** будет выполнено автоматическое тестирование установленных ДСЧ, перечень которых указан в окне «Управление датчиками случайных чисел» (см. Рисунок 40). При тестировании БиоДСЧ пользователю потребуется выполнить указанные в окне действия для генерации случайной последовательности.

Результаты тестирования установленных ДСЧ будут отражены в окне (см. Рисунок 48).

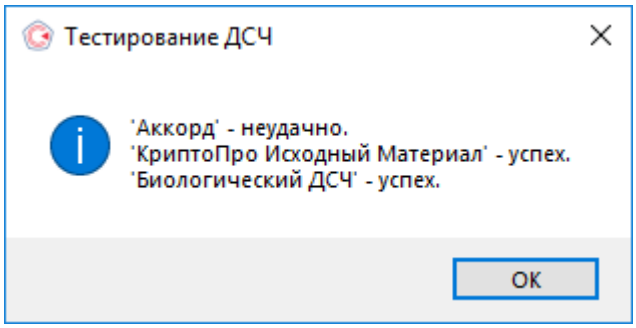


Рисунок 48. Тестирование ДСЧ

2.5 Работа с контейнерами и сертификатами

Вкладка **Сервис** панели управления СКЗИ КриптоПро CSP предназначена для выполнения следующих операций:

- Копирование и удаление закрытого ключа, находящегося в существующем контейнере;
- Тестирование (проверка работоспособности) и отображение свойств ключа (ключей) и сертификата (сертификатов) в существующем контейнере;
- Просмотр и установка сертификата, находящегося в существующем контейнере закрытого ключа на носителе;
- Осуществление связки между существующим сертификатом из файла и существующим контейнером закрытого ключа на носителе;
- Изменение и удаление сохраненных паролей (PIN-кодов) доступа к носителям закрытых ключей;
- Удаление информации о ранее использованных съёмных носителях, на которых располагались контейнеры закрытых ключей.

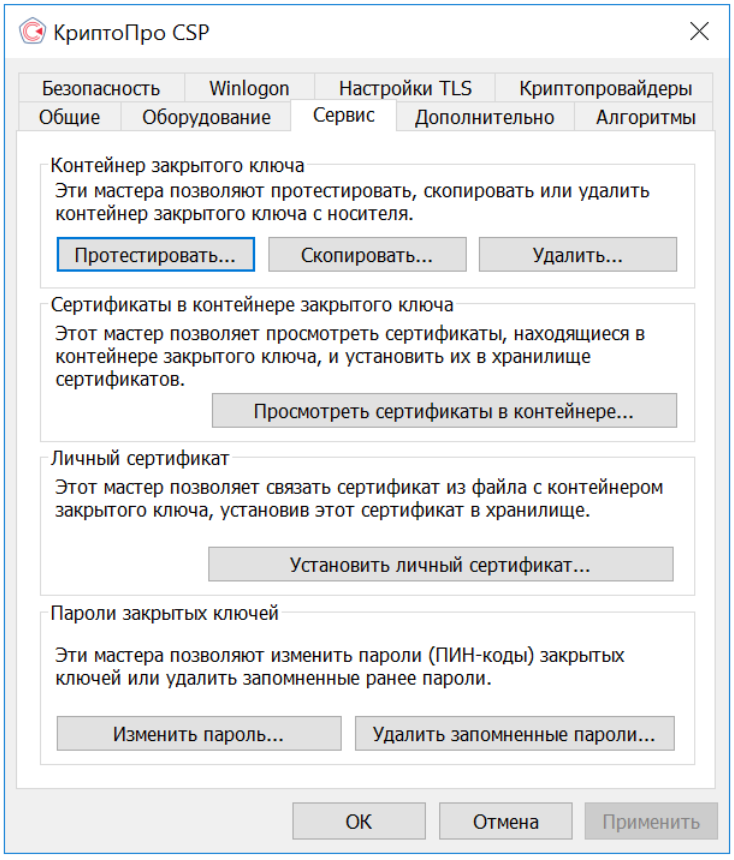


Рисунок 49. Вкладка **Сервис** панели управления

2.5.1 Тестирование, копирование и удаление контейнера закрытого ключа

2.5.1.1 Тестирование контейнера закрытого ключа

Для проведения тестирования работоспособности контейнера закрытого ключа откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Протестировать**. Откроется окно «Тестирование контейнера закрытого ключа» (см. Рисунок 50).

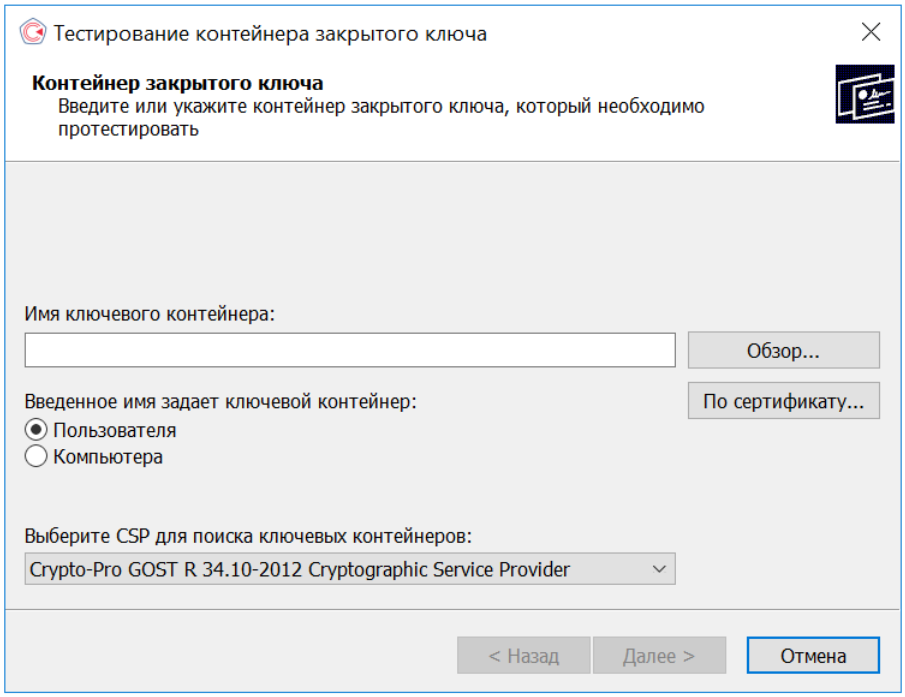


Рисунок 50. Тестирование контейнера закрытого ключа

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см. Рисунок 52).

Для поиска имени контейнера доступны следующие опции:

- **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для тестирования контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

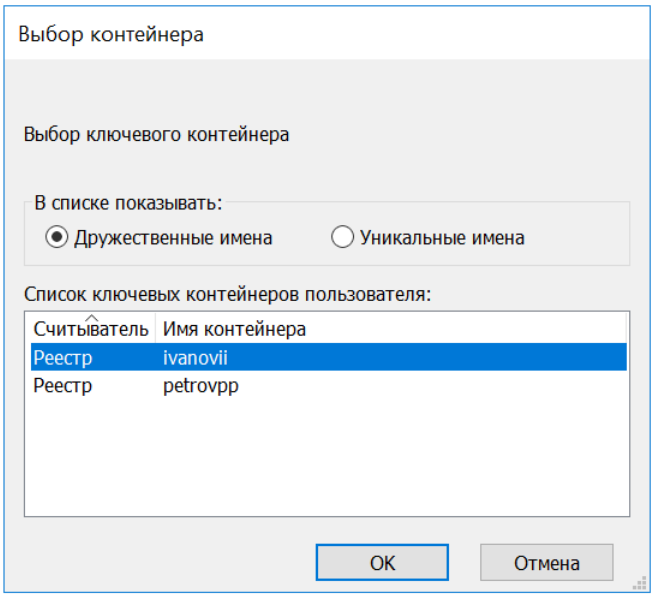


Рисунок 51. Выбор ключевого контейнера

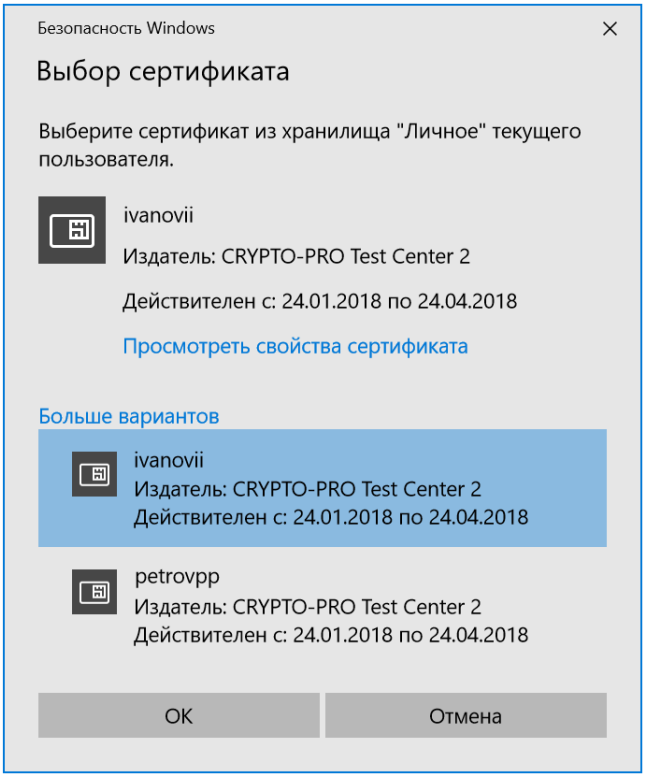


Рисунок 52. Выбор сертификата

После заполнения всех полей нажмите кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **OK**. После этого откроется форма с результатом тестирования (см. Рисунок 53), в котором будут выведены информация о данном контейнере и результат теста.

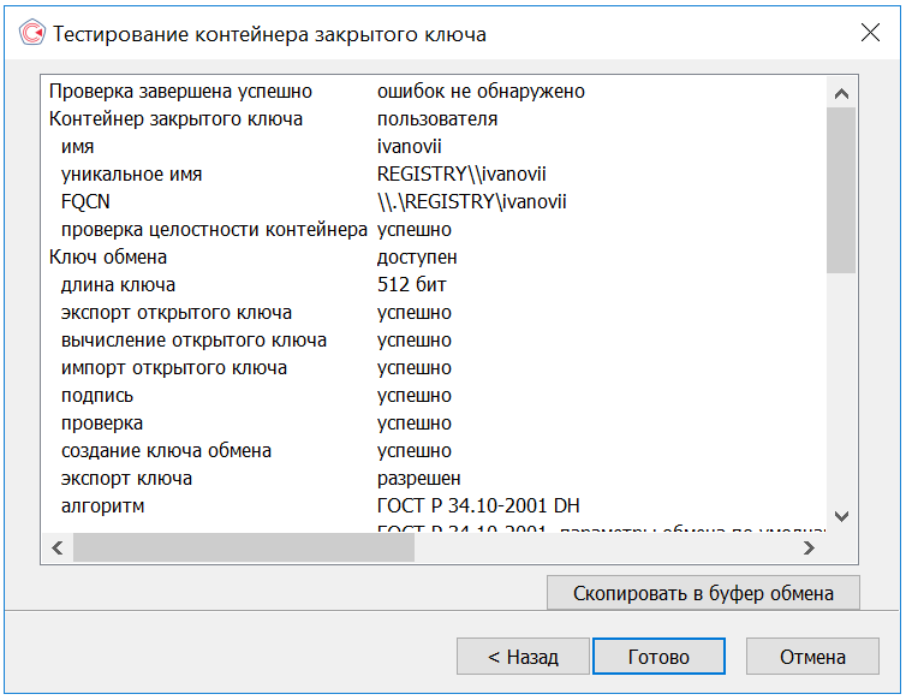


Рисунок 53. Окно с результатами тестирования контейнера

2.5.1.2 Копирование контейнера закрытого ключа

Для копирования контейнера закрытого ключа откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Скопировать**. Откроется окно «Копирование контейнера закрытого ключа» (см. Рисунок 54).

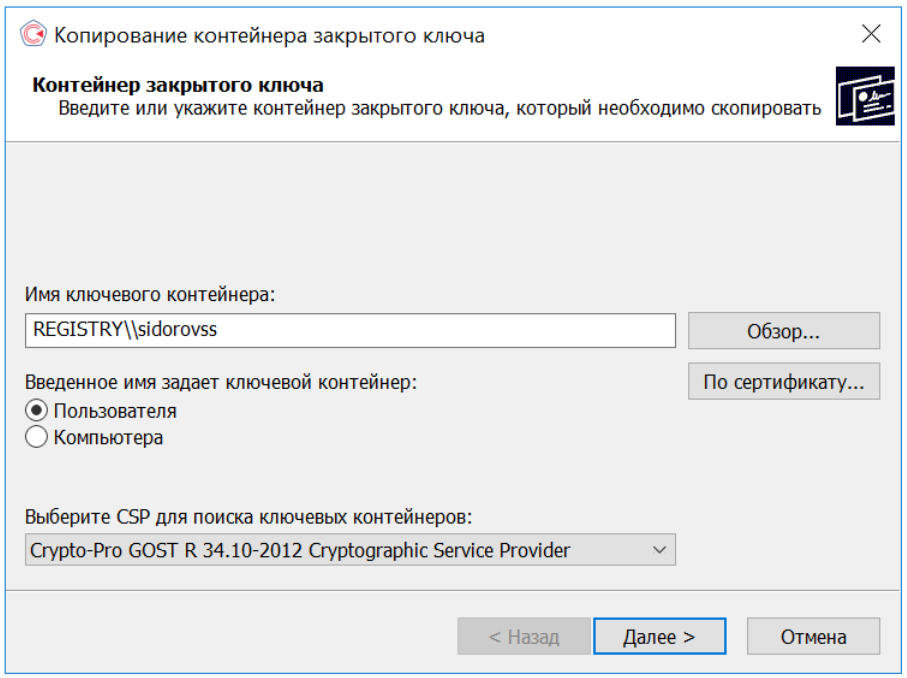


Рисунок 54. Копирование контейнера закрытого ключа

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см.

Рисунок 52).

Для поиска имени контейнера доступны следующие опции:

• **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для работы с контейнером закрытого ключа из хранилища Локального компьютера необходимы права администратора.

• **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После заполнения всех полей нажмите кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **OK**.

Откроется окно ввода параметров нового контейнера закрытого ключа (см. Рисунок 55). Введите имя нового ключевого контейнера и установите переключатель **Введенное имя задает ключевой контейнер** в положение **Пользователь** или **Компьютер**, в зависимости от того, в каком хранилище требуется разместить скопированный контейнер.

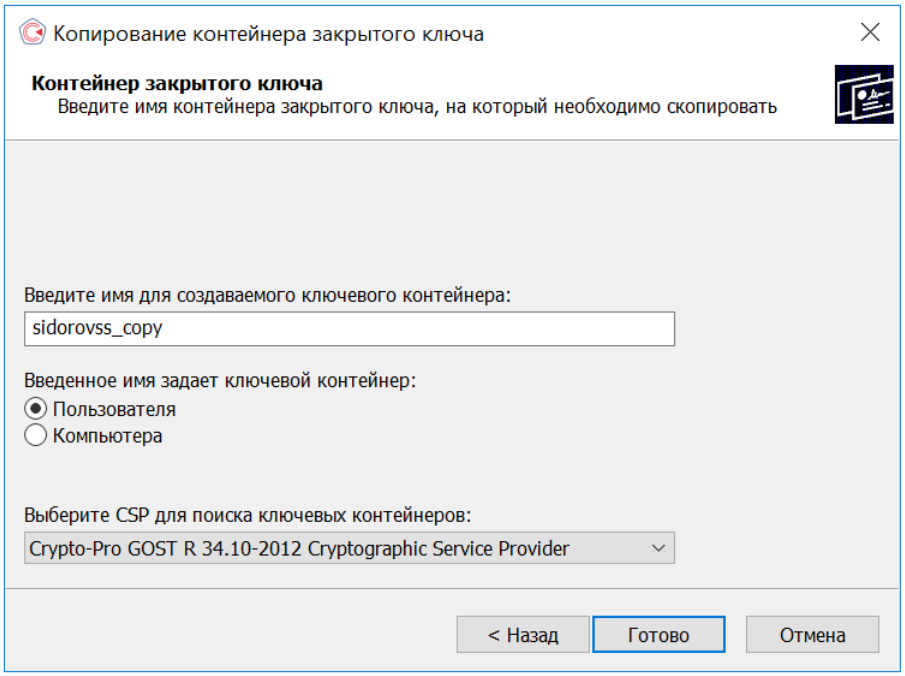


Рисунок 55. Ввод имени нового контейнера

После ввода параметров контейнера нажмите кнопку **Готово**. Откроется окно, в котором необходимо выбрать носитель для скопированного контейнера (см. Рисунок 56).

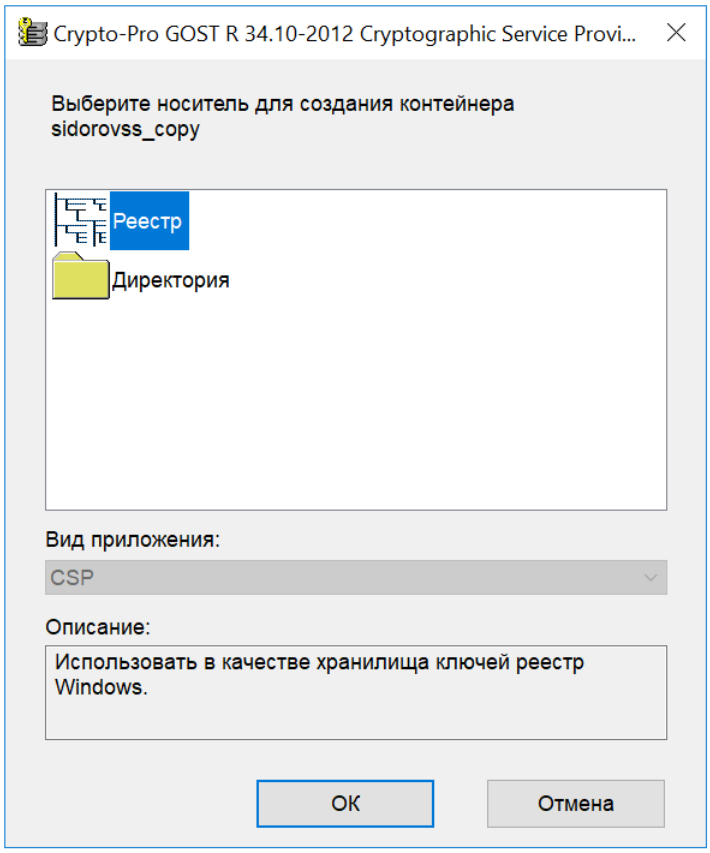


Рисунок 56. Выбор носителя для нового контейнера

Вставьте носитель в считыватель, выберите носитель из перечня устройств и нажмите кнопку **OK**. Откроется окно создания пароля на доступ к закрытому ключу (см. Рисунок 57). Введите пароль и подтвердите его.

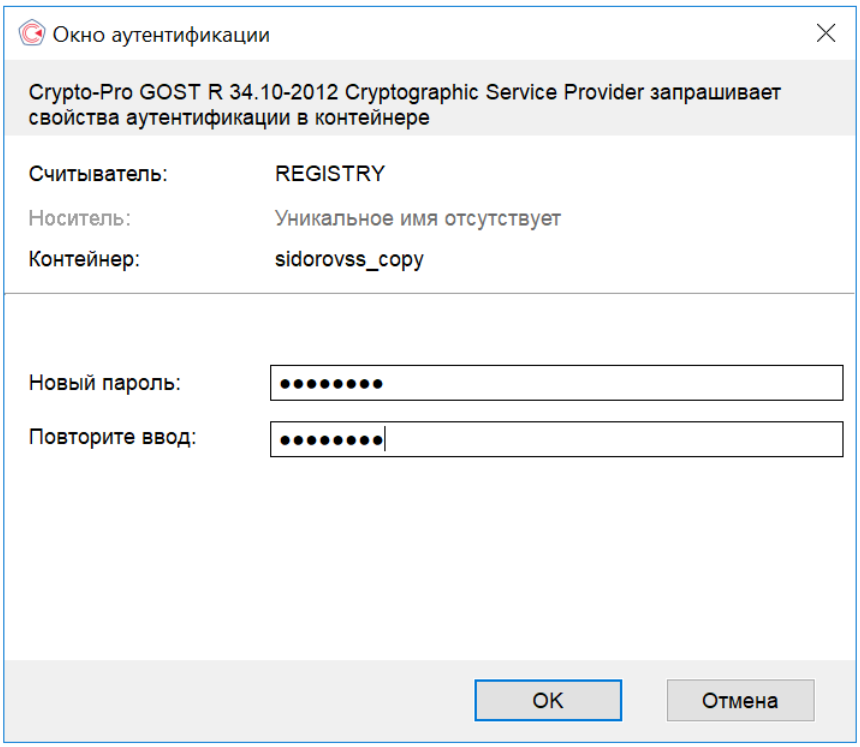


Рисунок 57. Ввод пароля для нового контейнера

После ввода необходимых данных нажмите кнопку **OK** для запуска процедуры копирования контейнера закрытого ключа.

В случае ошибки копирования контейнера (например, если при создании ключа он не был отмечен как экспортируемый) при выборе контейнера и нажатии на кнопку **Далее** открывается окно с ошибкой копирования контейнера (см. Рисунок 58).

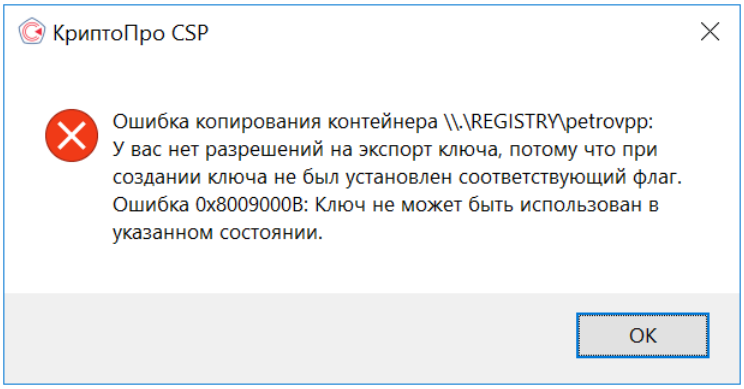


Рисунок 58. Ошибка при копировании контейнера

2.5.1.3 Удаление контейнера закрытого ключа

Для удаления контейнера закрытого ключа откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Удалить контейнер**. Откроется окно «Удаление контейнера закрытого ключа» (см. Рисунок 59).

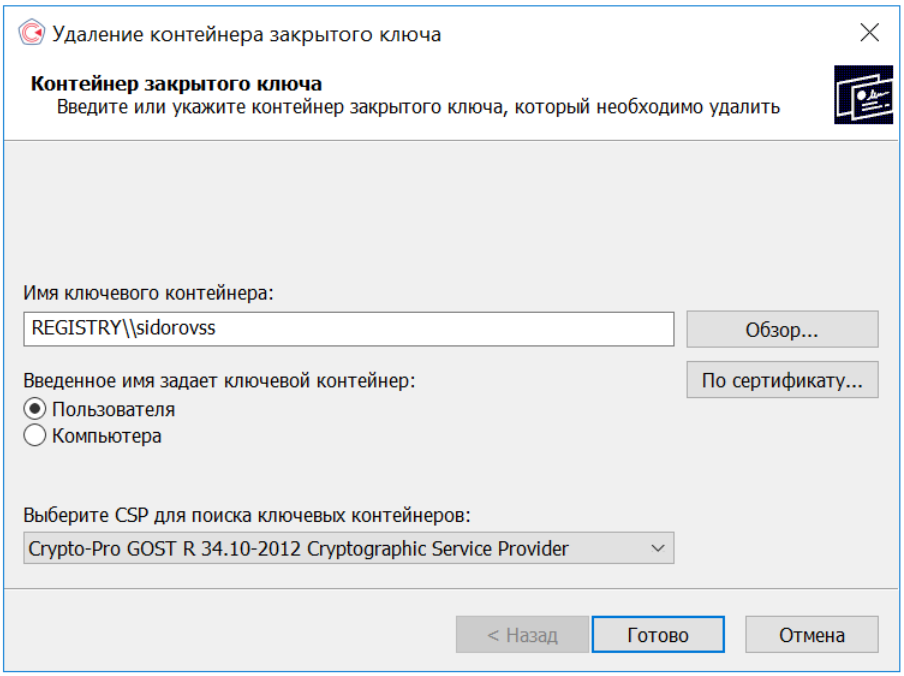


Рисунок 59. Удаление контейнера закрытого ключа

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см. Рисунок 52).

Для поиска имени контейнера доступны следующие опции:

- **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для удаления контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После заполнения всех полей нажмите кнопку **Готово**. Откроется окно подтверждения удаления ключевого контейнера (см. Рисунок 60), нажмите кнопку **Да** для продолжения.

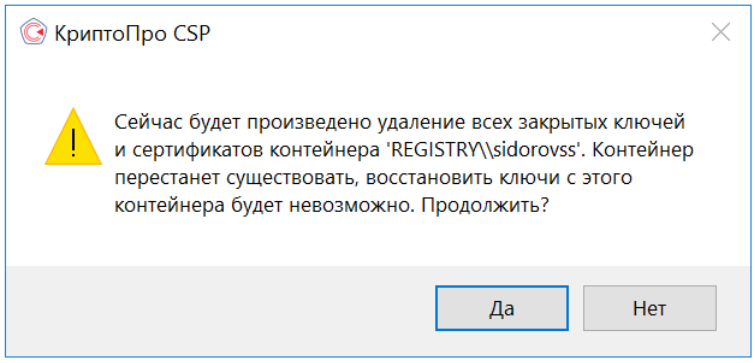


Рисунок 60. Окно подтверждения удаления ключевого контейнера

В случае наличия связанных с контейнером сертификатов в системных хранилищах после удаления ключевого контейнера будет предложено также удалить сертификаты (см. Рисунок 61).

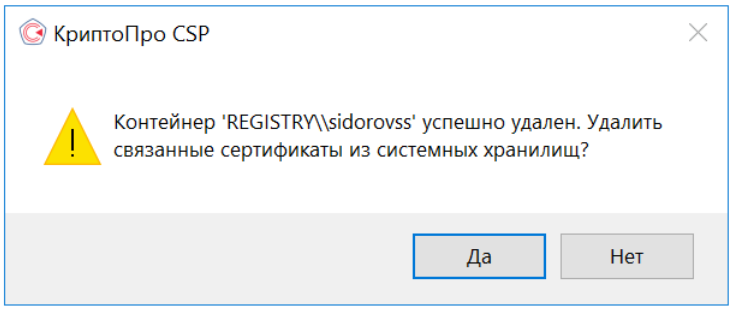


Рисунок 61. Окно подтверждения удаления связанных сертификатов

2.5.2 Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа

2.5.2.1 Просмотр сертификата, хранящегося в контейнере закрытого ключа

Для просмотра сертификата, хранящегося в контейнере закрытого ключа, откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Просмотреть сертификаты в контейнере**. Откроется окно «Сертификаты в контейнере закрытого ключа» (см. Рисунок 62).

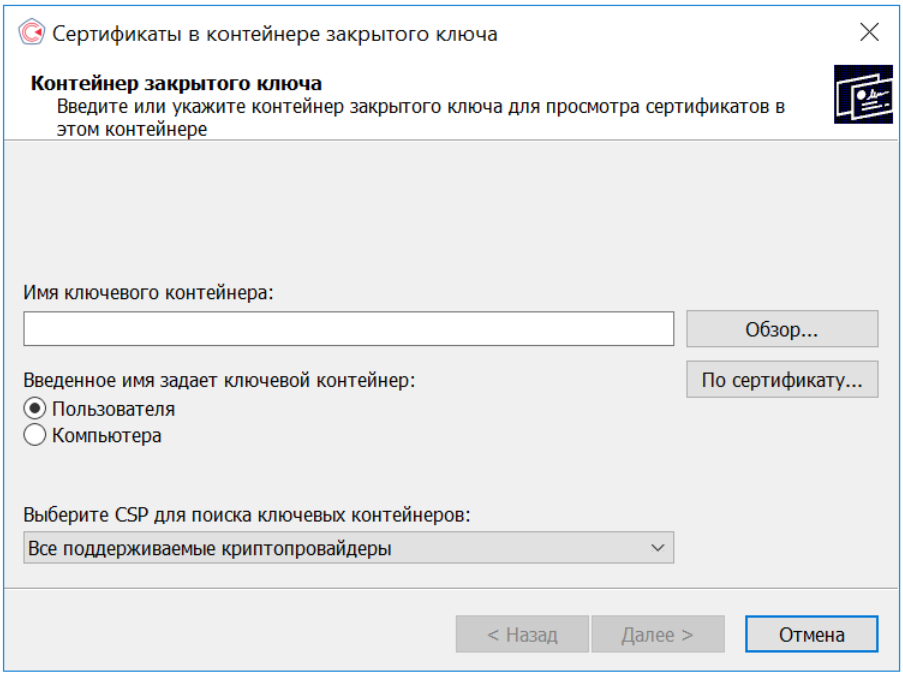


Рисунок 62. Сертификаты в контейнере закрытого ключа

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см. Рисунок 52).

Для поиска имени контейнера доступны следующие опции:

- **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Для просмотра контейнера закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После заполнения всех полей нажмите кнопку **Далее**. Если сертификата в контейнере закрытого ключа нет, откроется окно с предупреждением (см. Рисунок 63).

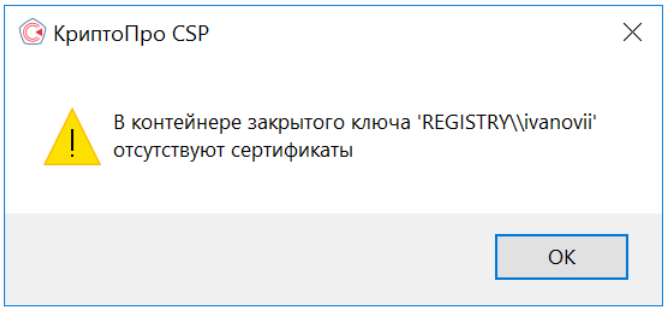


Рисунок 63. Окно, информирующее об отсутствии сертификата

Если в выбранном контейнере есть сертификат, откроется окно «Сертификат для просмотра» (см. Рисунок 64).

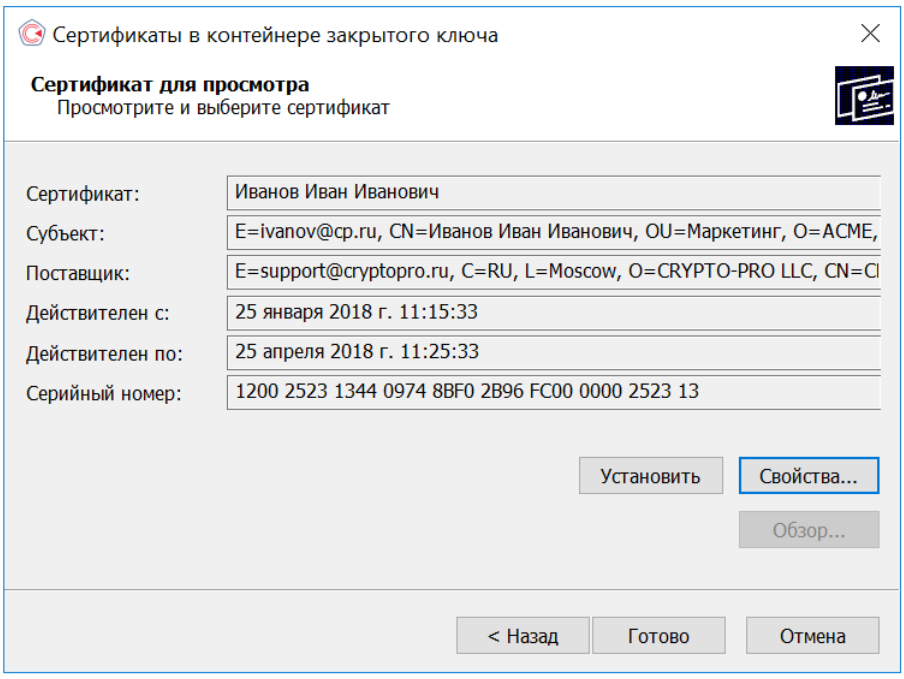


Рисунок 64. Просмотр сертификата в контейнере закрытого ключа

Для просмотра основных свойств сертификата нажмите кнопку **Свойства** в окне «Сертификаты в контейнере закрытого ключа» (см. Рисунок 64). Откроется окно просмотра свойств сертификата (см. Рисунок 65). На вкладке «Путь сертификации» можно просмотреть все сертификаты до корневого УЦ, если они содержатся в контейнере.

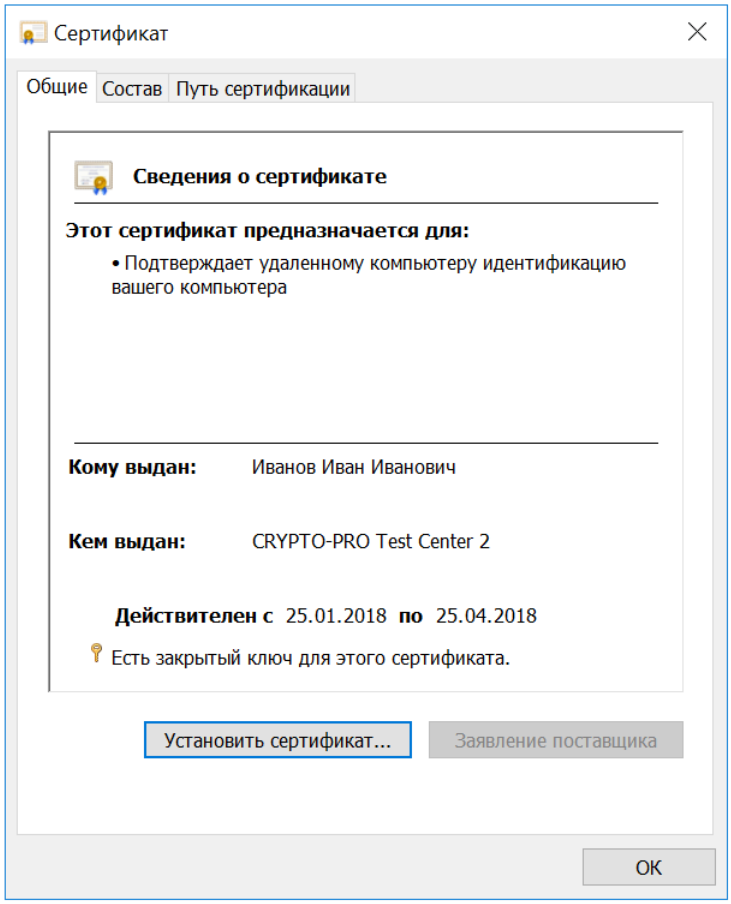


Рисунок 65. Окно просмотра свойств сертификата

2.5.2.2 Установка личного сертификата, хранящегося в контейнере закрытого ключа

Примечание. В данном разделе руководства под установкой личного сертификата понимается установка сертификата в хранилище **Личные** с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя как в локальном справочнике сертификатов компьютера, так и вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя, на другие рабочие места.

Для установки личного сертификата откройте его для просмотра. Для этого выполните последовательность действий, указанных в пункте 2.5.2.1.

В окне «Сертификаты в контейнере закрытого ключа» (см. Рисунок 64) нажмите кнопку **Установить**. Сертификат будет установлен в хранилище **Личные** текущего пользователя или компьютера, в зависимости от опции, выбранной при поиске контейнера. Если сертификат уже есть в хранилище, будет выдано предупреждение о перезаписи прежнего сертификата (см. Рисунок 66).

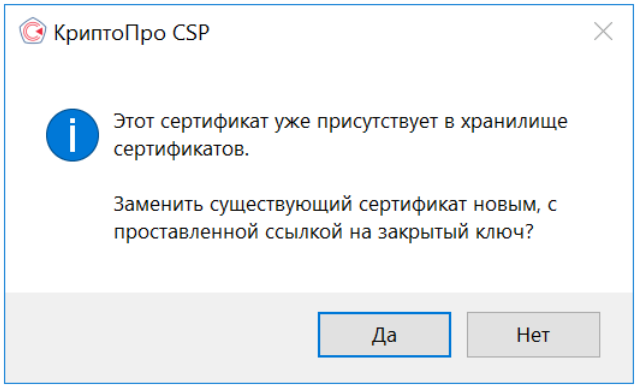


Рисунок 66. Предупреждение о перезаписи сертификата

В случае успеха появится сообщение о завершении операции (см. Рисунок 67).

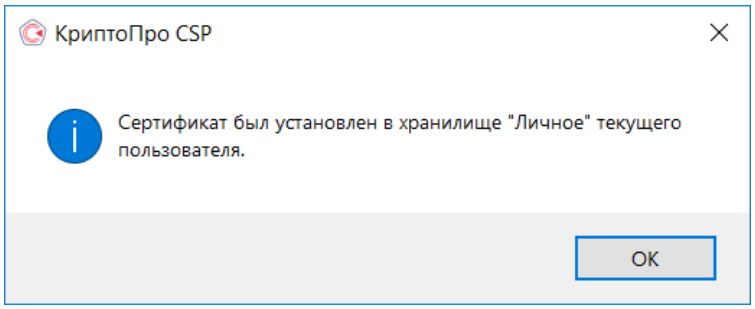


Рисунок 67. Окно завершения установки сертификата

При таком способе установки сертификатов в соответствующие хранилища также устанавливаются сертификаты корневых и промежуточных УЦ, если они содержатся в контейнере закрытого ключа.

2.5.3 Установка личного сертификата, хранящегося в файле

Для установки личного сертификата откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Установить личный сертификат**.

Запустится мастер установки личного сертификата. В окне «Расположение файла сертификата» (см. Рисунок 68) будет предложено указать **Имя файла сертификата**. Выберите путь к файлу с помощью кнопки **Обзор**, после чего нажмите кнопку **Далее**.

Примечание. Порядок действий и внешний вид окон мастера установки личного сертификата в случае импорта сертификата из файла обмена личной информацией в формате PKCS#12 описан в п. 2.5.3.1.

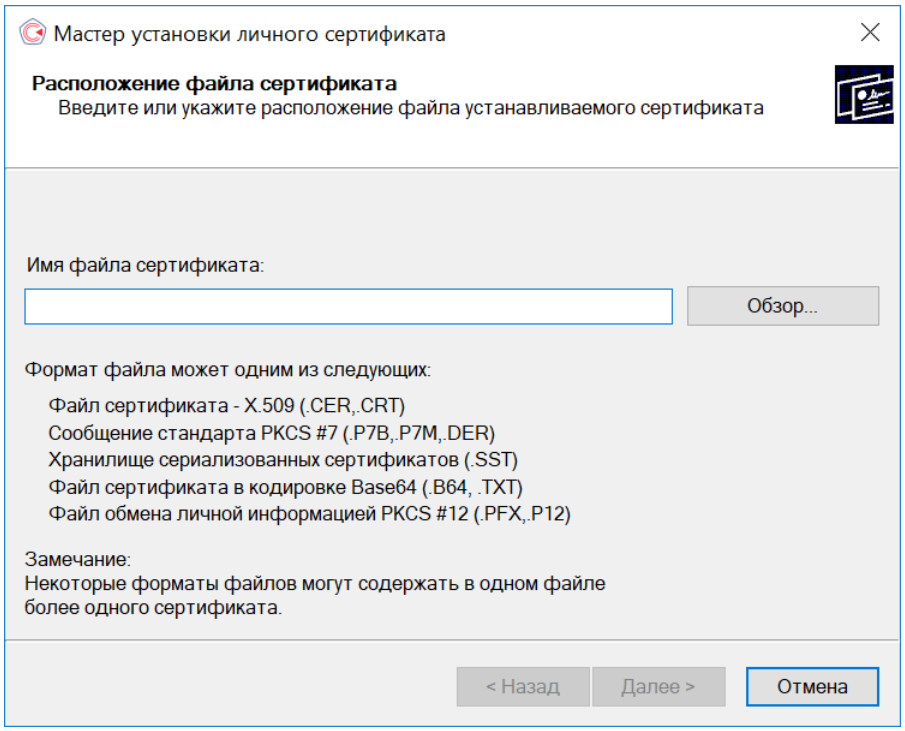


Рисунок 68. Выбор расположение файла сертификата

Откроется окно просмотра основной информации сертификата для установки (см. Рисунок 69). Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

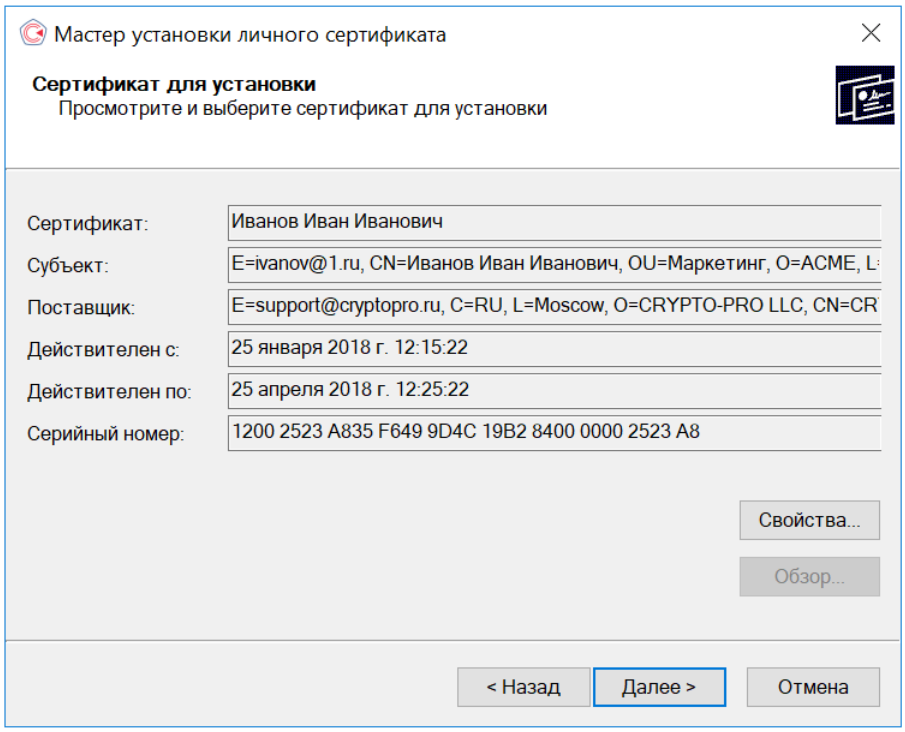


Рисунок 69. Просмотр сертификата для установки

Нажмите кнопку **Далее**. Откроется окно «Контейнер закрытого ключа» (см. Рисунок 70).

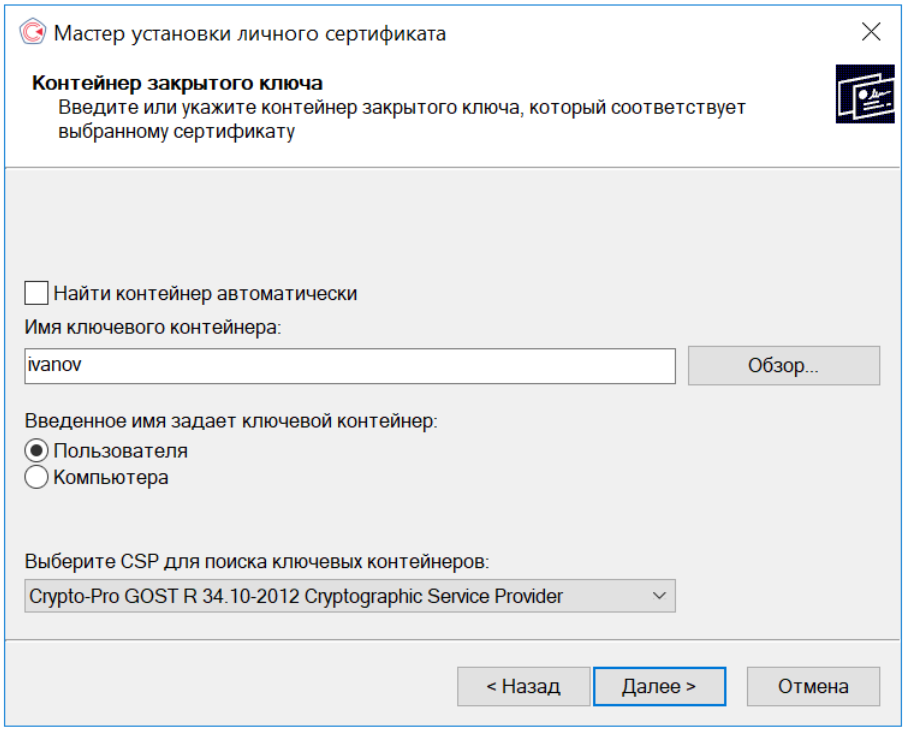


Рисунок 70. Выбор контейнера закрытого ключа

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см. Рисунок 52). Для автоматического поиска подходящего контейнера среди доступных можно воспользоваться опцией **Найти контейнер автоматически**.

Для поиска имени контейнера доступны следующие опции:

- **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер.
- **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После заполнения всех полей нажмите кнопку **Далее**. Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **OK**.

На следующем шаге с помощью кнопки **Обзор** выберите хранилище для установки сертификата (см. Рисунок 71). Сертификат будет установлен в хранилище пользователя или компьютера, в зависимости от расположения контейнера закрытого ключа (см. Рисунок 70).

Одновременно сертификат можно записать в ключевой контейнер для удобства поиска сертификата при переносе контейнера на другой компьютер. Для этого служит поле **Установить сертификат в контейнер**. Для записи в контейнер всей цепочки сертификатов установите в поле знак галочки ☑, для записи только импортируемого сертификата — знак квадрата ▣.

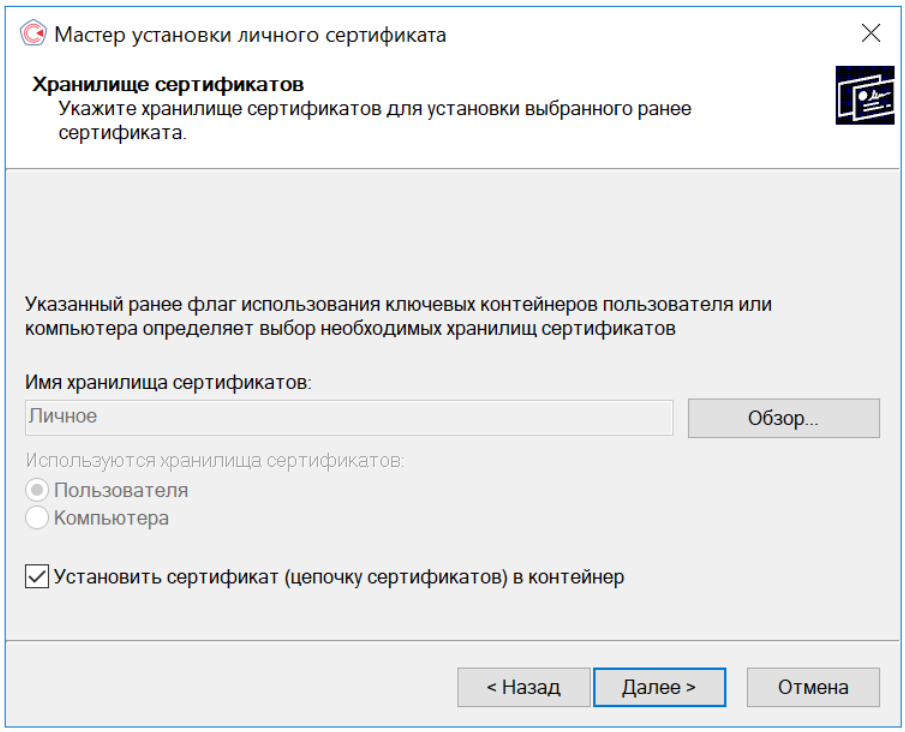


Рисунок 71. Выбор хранилища сертификатов

На последнем шаге мастера установки личного сертификата нужно проверить правильность указанных параметров и для выполнения установки сертификата нажать кнопку **Готово** (см. Рисунок 72).

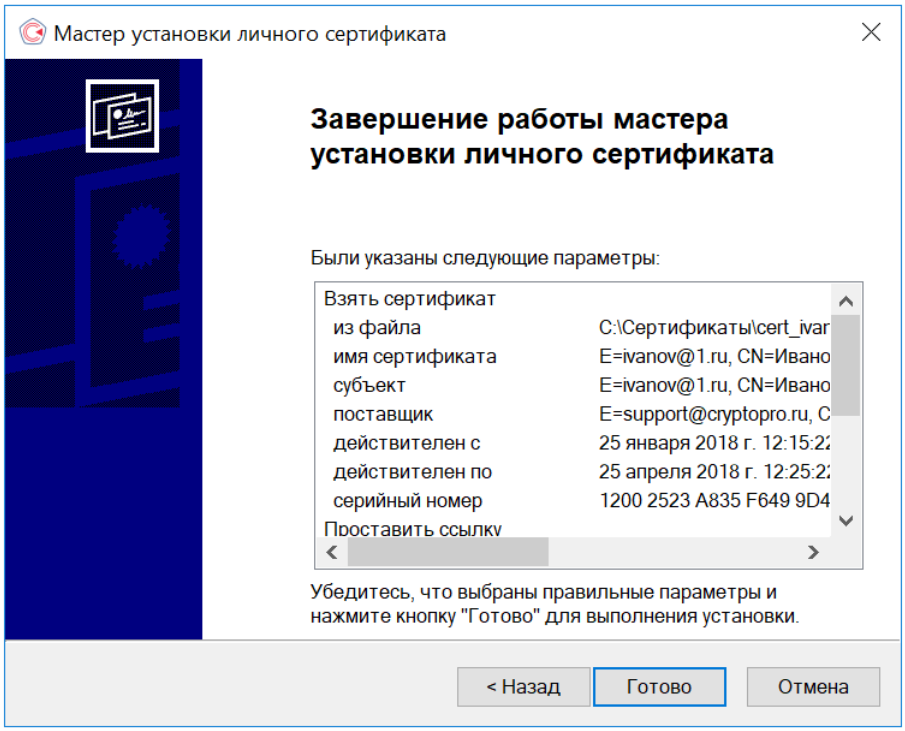


Рисунок 72. Завершение работы мастера установки личного сертификата

По окончанию операции откроется окно с сообщением об ее успешном выполнении или сведениями о возникшей ошибке.

2.5.3.1 Установка сертификата из файла формата PKCS#12

В случае установки сертификата из файла обмена личной информацией PKCS#12 откроется специальное окно (см. Рисунок 73). Введите пароль для PFX-файла и установите необходимые параметры импорта сертификата:

• опция **Использовать локальное хранилище компьютера для сертификата** доступна только при запуске панели с правами администратора

• опция **Установить сертификат (цепочку сертификатов) в контейнер** позволяет установить в ключевой контейнер сертификат или цепочку сертификатов для удобства поиска сертификата при переносе контейнера. Для записи в контейнер всей цепочки сертификатов установите в поле знак галочки ☑, для записи только импортируемого сертификата — знак квадрата ■.

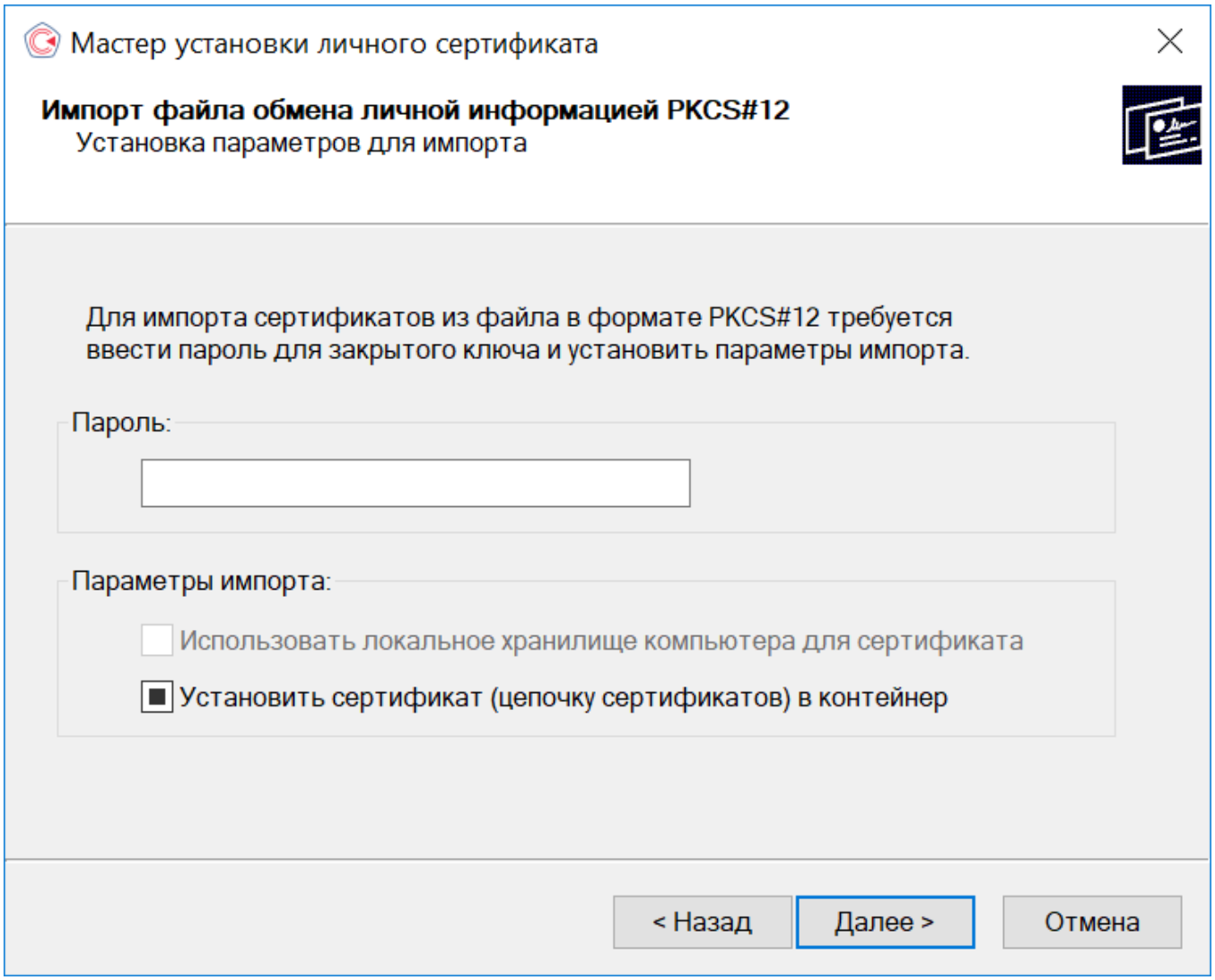


Рисунок 73. Установка сертификата из файла формата PKCS#12

На следующем шаге мастера установки личного сертификата проверьте правильность указанных параметров и нажмите кнопку **Готово** (см. Рисунок 72). После этого начнется процесс создания нового ключевого контейнера для закрытого ключа из файла обмена личной информацией (подробнее см. Создание ключевого контейнера). По окончанию операции откроется окно с сообщением об ее успешном выполнении или сведениями о возникшей ошибке.

2.5.4 Управление паролями доступа к закрытым ключам

2.5.4.1 Изменение пароля на доступ к закрытому ключу

Для изменения пароля контейнера закрытого ключа откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Изменить пароль**. Откроется окно «Контейнер закрытого ключа» (см. Рисунок 74).

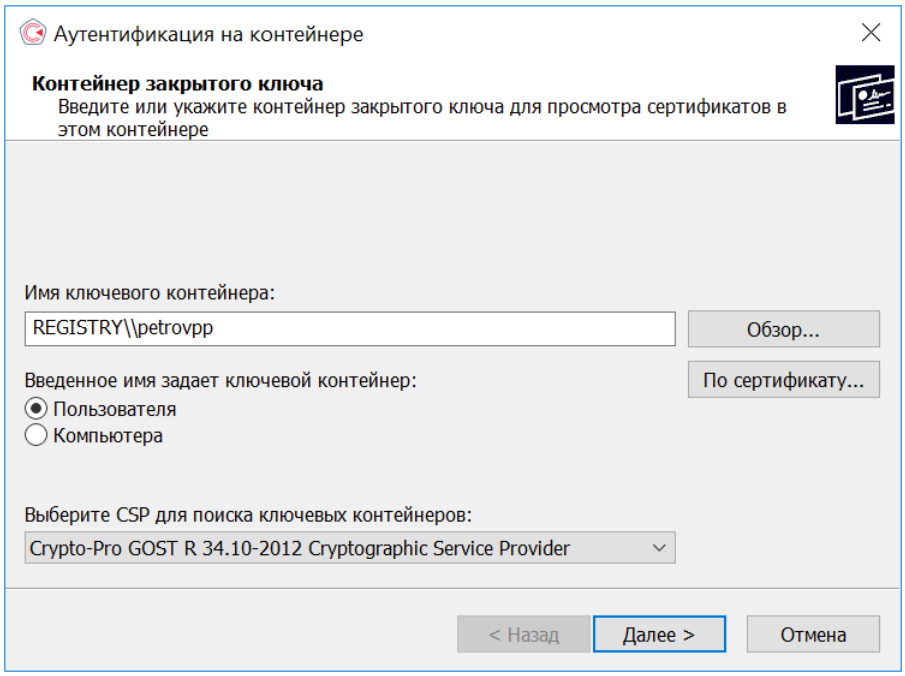


Рисунок 74. Выбор контейнера закрытого ключа для изменения пароля

На этой форме необходимо заполнить поле **Имя ключевого контейнера**. Оно может быть введено вручную или найдено в списках контейнеров (кнопка **Обзор**, см. Рисунок 51) или сертификатов (кнопка **По сертификату**, см. Рисунок 52).

Для поиска имени контейнера доступны следующие опции:

- **Введенное имя задает ключевой контейнер** — переключатель устанавливается в положение **Пользователь** или **Компьютер** в зависимости от того, в каком хранилище (Личные или Локального компьютера соответственно) расположен контейнер. Переключатель автоматически ставится в нужное положение, если выбор производился по сертификату. Для работы с контейнером закрытого ключа из хранилища Локального компьютера необходимы права администратора.
- **Выберите CSP для поиска ключевых контейнеров** — необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После заполнения всех полей нажмите кнопку **Готово**. Откроется окно ввода пароля на доступ к закрытому ключу выбранного контейнера (см. Рисунок 75). Введите пароль и нажмите кнопку **OK**.

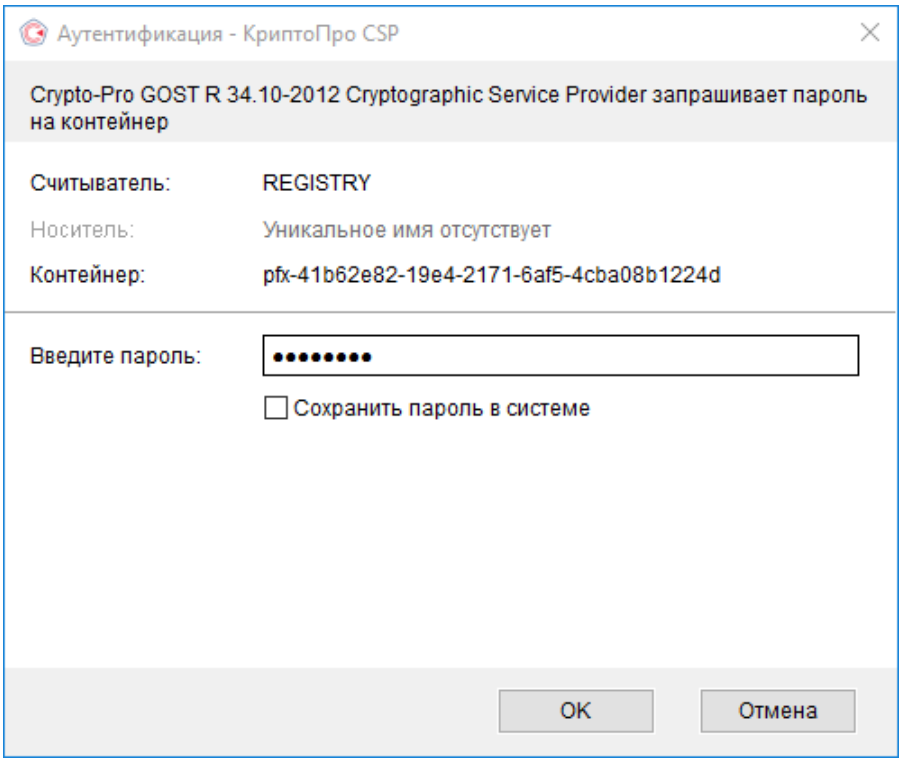


Рисунок 75. Ввод пароля на доступ к контейнеру

Если пароль введен верно, откроется окно ввода нового пароля на доступ к закрытому ключу (см. Рисунок 76). Введите дважды новый пароль и нажмите кнопку **OK**.

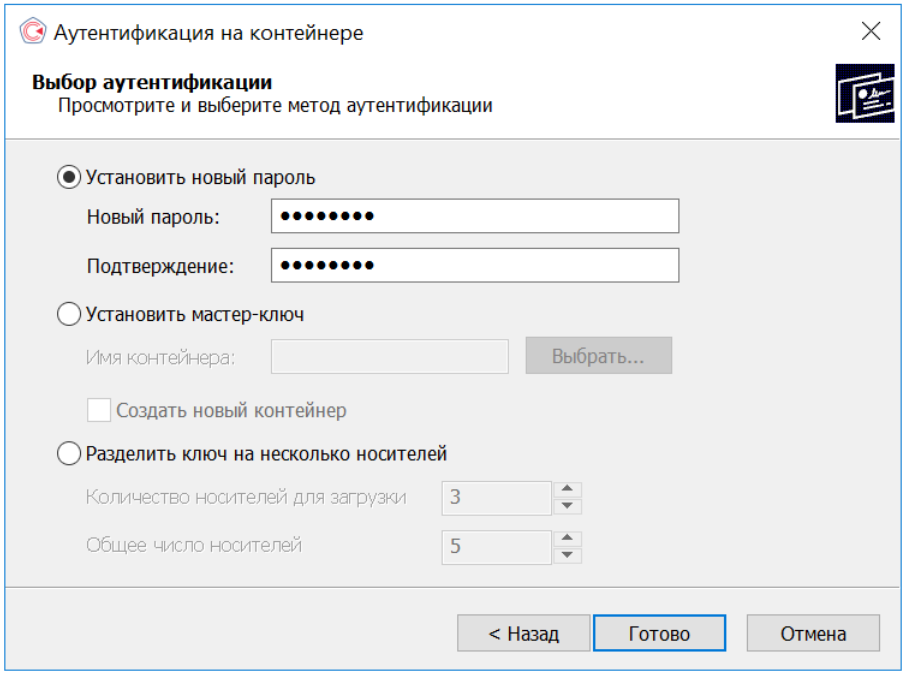


Рисунок 76. Ввод нового пароля на доступ к контейнеру

После подтверждения ввода будет установлен новый пароль на доступ к закрытому ключу. Более подробно работа по установке пароля и дополнительных параметров защиты контейнера описана в пункте Выбор способа защиты доступа к закрытому ключу.

Примечание. Вместо установки пароля на доступ к закрытому ключу СКЗИ КриптоПро CSP позволяет зашифровать данный закрытый ключ на другом закрытом ключе, а также разделить закрытый ключ на несколько ключевых носителей. Подробнее об этом в разд. 3.2.4

2.5.4.2 Сохранение пароля на доступ к закрытому ключу

СКЗИ КриптоПро CSP позволяет сохранить в специальном хранилище локального компьютера пароли на доступ к контейнеру закрытого ключа. Когда пароль сохранен, при обращении к закрытому ключу он не запрашивается. В это же хранилище записывается точный путь к ключевому контейнеру (связка между именем контейнера и уникальным именем контейнера).

Для сохранения пароля необходимо установить флаг **Сохранить пароль в системе** в окне ввода пароля на доступ к закрытому ключу (см. Рисунок 75).

Если сохранение пароля контейнера запрещено групповой политикой «Запретить использование сохраненных паролей», флаг **Сохранить пароль в системе** недоступен для изменения. При установке флага **Требовать пароль при каждой операции** пароль носителя будет запрашиваться при каждой операции (подробнее см. ЖТЯИ.00101-02 91 02. Руководство администратора безопасности Windows).

2.5.4.3 Удаление запомненных паролей

Для удаления запомненного пароля откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 49). Нажмите кнопку **Удалить запомненные пароли**. Откроется окно «Удаление запомненных паролей» (см. Рисунок 77).

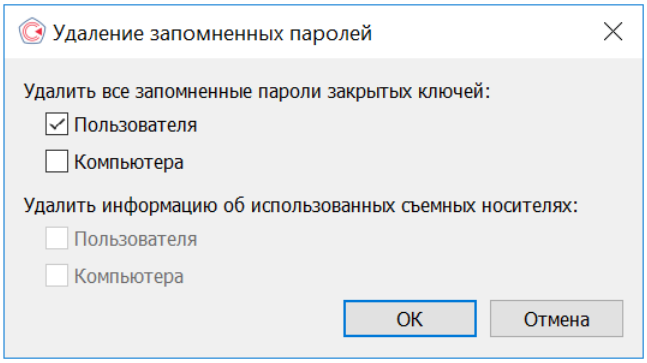


Рисунок 77. Удаление запомненных паролей

В этом окне установите флаги **Пользователя/Компьютера** для удаления сохраненных на локальном компьютере в специальном хранилище паролей и нажмите кнопку OK. Если сохраненных паролей нет, то соответствующая область будет затемнена.

СКЗИ КриптоПро CSP осуществит удаление сохраненных паролей только из специального хранилища на локальном компьютере; пароль на доступ к закрытому ключу не удаляется.

Кроме того, в этом же окне можно отдельно удалить информацию о физических характеристиках носителей, на которых расположены ключевые контейнеры, использовавшиеся ранее на данном компьютере. Это полезно, если ключевой контейнер на новом носителе имеет то же имя, что один из ранее использовавшихся на данном компьютере контейнеров.

2.6 Установка параметров безопасности

Вкладка **Безопасность** контрольной панели СКЗИ КриптоПро CSP предназначена для выбора параметров безопасности при работе с СКЗИ КриптоПро CSP.

Для установки параметров безопасности откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора»

на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Безопасность** (см. Рисунок 78).

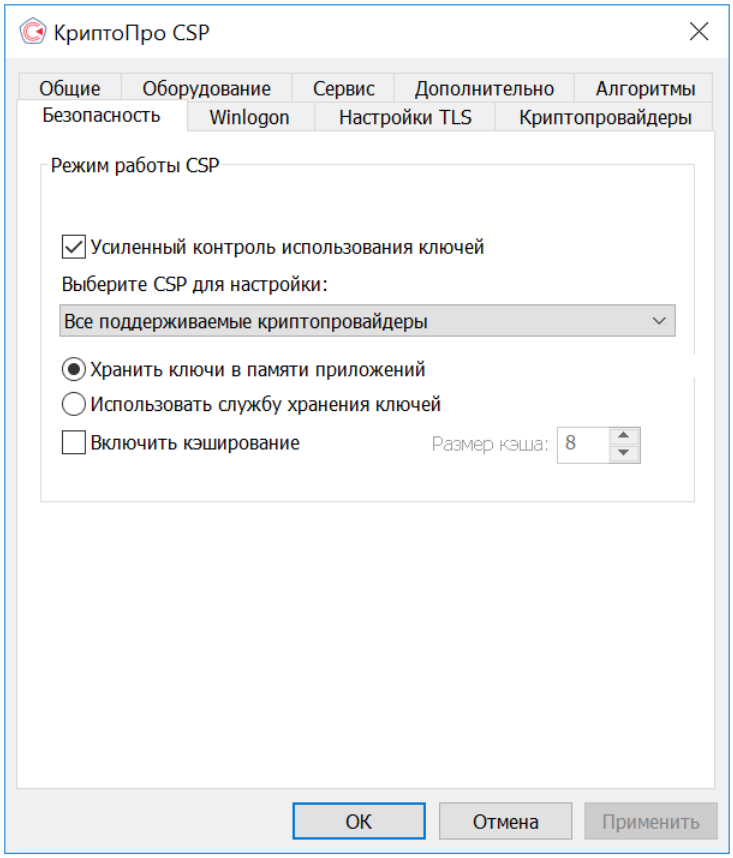


Рисунок 78. Вкладка **Безопасность** панели управления

На вкладке **Безопасность** можно включить режим усиленного контроля использования ключей, если он не был включен при установке СКЗИ КриптоПро CSP. После включения режима через контрольную панель **в обязательном порядке необходимо**:

1) установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера *CryptoProTrustedStore* («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки **Сертификаты** либо с помощью утилиты `certmgr.exe`:

```
certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file <имя файла сертификата>
```

2) перезагрузить компьютер.

На вкладке **Безопасность** можно выбрать режим работы криптопровайдера с хранением ключей в памяти приложений или с хранением ключей в службе хранения ключей. При хранении ключей в службе хранения ключей все операции с закрытым ключом производятся внутри службы, внешнему приложению выдается только результат, что более безопасно, чем хранить ключи непосредственно в памяти приложений.

Для СКЗИ КриптоПро CSP, сертифицированного по уровню КС1, служба хранения ключей по умолчанию не устанавливается и выбор соответствующего режима на вкладке **Безопасность** недоступен. В случае необходимости использования службы хранения ключей она может быть установлена дополнительно. Для этого на вкладке **Безопасность** нажмите на кнопку **Установить** (см. Рисунок 79) и дождитесь завершения установки компонента.

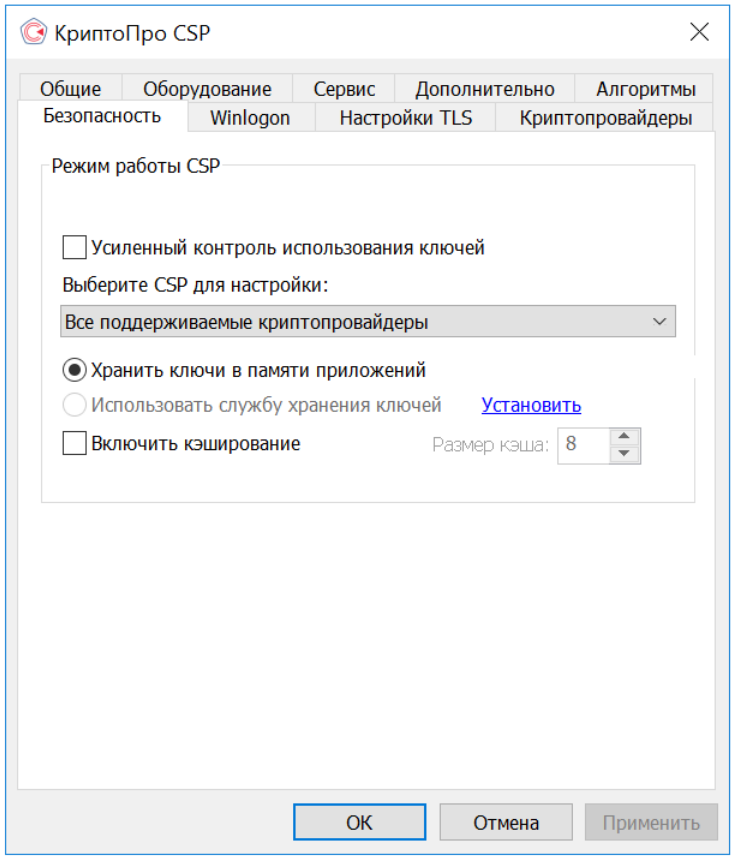


Рисунок 79. Установка службы хранения ключей

2.6.1 Кэширование контейнеров закрытых ключей

При хранении ключей в службе хранения ключей возможно применение кэширования контейнеров закрытых ключей (только для пассивных хранилищ ключевой информации без использования криптографических механизмов, реализованных на смарт-карте/токене). Кэширование заключается в том, что считанные с носителя ключи остаются в памяти сервиса.

Такой ключ доступен после завершения работы загрузившего этот ключ приложения. Также ключ из кэша может быть доступен и после извлечения ключевого носителя из считывателя, для этого необходимо добавить параметр реестра AllowWorkWithoutCarrier со значением «1» в ветку `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CryptoPro\Cryptography\CurrentVersion\Parameters`.

Каждый ключ из кэша доступен любому приложению, которое работает под той же учётной записью, что и приложение, поместившее этот ключ в кэш. Все ключи из кэша доступны до завершения работы службы хранения ключей. При переполнении кэша очередной ключ записывается на место самого раннего ключа, помещённого в кэш.

Кэширование контейнеров позволяет увеличить производительность приложений за счет более быстрого доступа к закрытому ключу, т.к. считывание ключа осуществляется только один раз.

Для включения режима кэширование установите флаг в поле **Включить кэширование**. Необходимо также задать размер кэша в соответствующем поле ввода. Размер кэша задает количество ключей, которые одновременно могут храниться в памяти.

Примечание. Если на доступ к закрытому ключу установлен пароль, пароль не сохранен на локальном компьютере и закрытый ключ находится в кэше (ранее к нему уже был осуществлен доступ), то обращение к данному закрытому ключу произойдет без появления окна ввода пароля пользователя – ключ автоматически считывается из кэша.
СКЗИ КриптоПро CSP осуществляет кэширование закрытых ключей, связанных с сертификатами, установленными в хранилище сертификатов Локального компьютера (например, закрытых ключей Центра сертификации, Web-сервера) только для конкретного пользователя.

2.7 Дополнительные настройки

Вкладка **Дополнительно** контрольной панели СКЗИ КриптоПро CSP предназначена для:
- просмотра версий и путей размещения используемых СКЗИ КриптоПро CSP файлов;
- пересчета контрольных сумм системных библиотек ОС;
- установки времени ожидания ввода информации от пользователя.

2.7.1 Просмотр версий используемых файлов

Для просмотра версий и путей размещения используемых СКЗИ КриптоПро CSP файлов откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Дополнительно** (см. Рисунок 80).

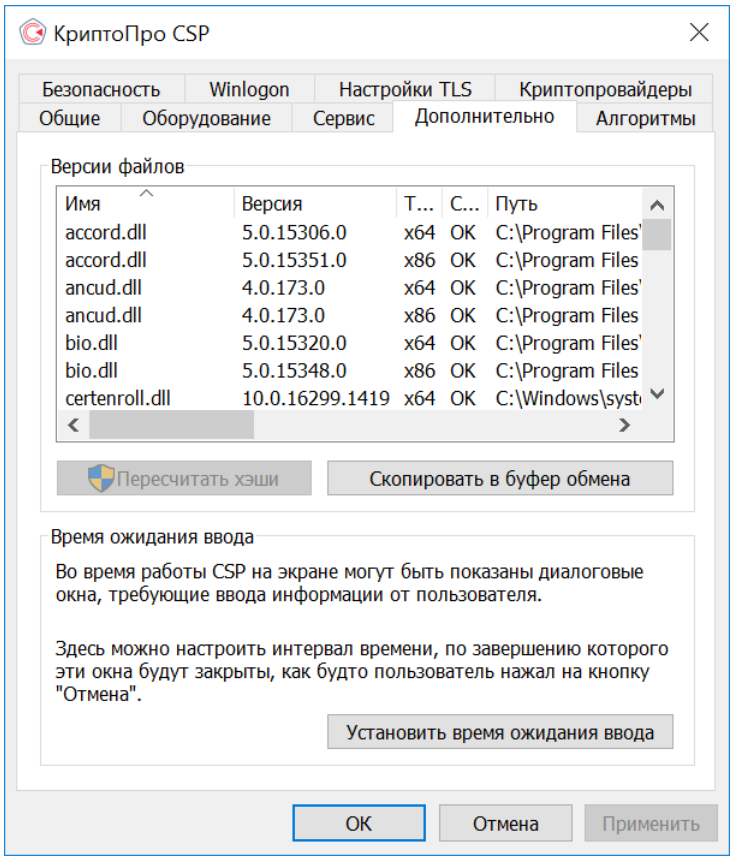


Рисунок 80. Вкладка **Дополнительно** панели управления

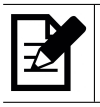
В разделе **Версии файлов** в табличной форме представлена информация о версиях и путях размещения использующихся СКЗИ КриптоПро CSP файлов. Данную информацию можно скопировать в буфер обмена, нажав на соответствующую кнопку.

2.7.2 Пересчет контрольных сумм системных библиотек ОС

КриптоПро CSP контролирует целостность некоторых библиотек операционной системы Microsoft Windows, которые могут заменяться при установке обновлений ОС. Для корректной работы СКЗИ после обновления ОС необходимо пересчитать контрольные суммы системных библиотек.

Для этого откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Дополнительно** (см. Рисунок 80) и нажмите кнопку **Пересчитать хэши**.

Необходимо проконтролировать, что изменены контрольные суммы только следующих системных библиотек:
- certenroll.dll
- crypt32.dll
- cryptsp.dll
- inetcomm.dll
- kerberos.dll
- rastls.dll
- schannel.dll
- sspicli.dll
- wininet.dll



Примечание. Кнопка «Пересчитать хэши» активна только в случае обновления системных библиотек ОС, перечисленных выше.

2.7.3 Установка времени ожидания ввода информации от пользователя

Во время работы СКЗИ КриптоПро CSP на экране могут появляться диалоговые окна, требующие ввода пользователем определенных данных (например, ввод пароля на доступ к закрытому ключу).

Для того, чтобы установить интервал времени, по завершении которого эти окна будут автоматически закрыты (действие, эквивалентное нажатию пользователем кнопки **Отмена**), откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Дополнительно** (см. Рисунок 80). Нажмите кнопку **Установить время ожидания ввода**.

Откроется окно «Интервал времени ожидания ввода» (см. Рисунок 81).

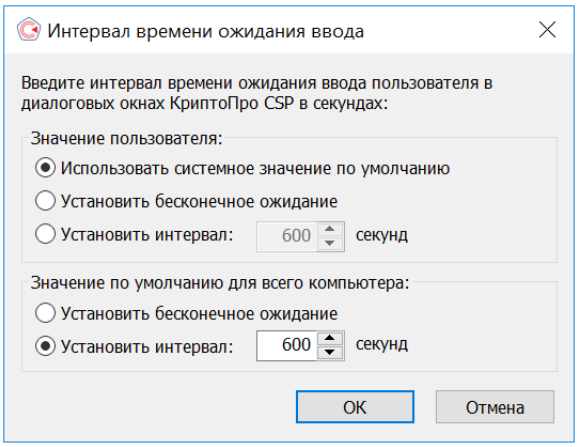


Рисунок 81. Установка интервала времени ожидания ввода

В этом окне установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

Переключатель **Значение пользователя** можно установить в одно из следующих положений:

• Использовать системное значение по умолчанию – устанавливает значение, определенное переключателем Значение по умолчанию для всего компьютера; это значение установлено по умолчанию;
• Установить бесконечное ожидание – устанавливает бесконечное ожидание ввода данных пользователя;
• Установить интервал – определяет интервал времени, во время которого пользователь должен ввести данные.

Изменить переключатель **Значение по умолчанию** для всего компьютера может только администратор локального компьютера. При этом если в панели КриптоПро CSP активна ссылка «Запустить с правами администратора» (см. Рисунок 18), то её нужно нажать.

По умолчанию установлено ожидание ввода в течение 600 секунд.

Примечание. Значение пользователя имеет больший приоритет по отношению к **Значению по умолчанию для всего компьютера** (например, если значение переключателя **Значение по умолчанию для всего компьютера** установлено в положение *Установить интервал 600 секунд*, а переключатель **Значение пользователя** в положение *Установить бесконечное ожидание*, то действительным будет значение *Установить бесконечное ожидание*).

2.8 Выбор параметров криптографических алгоритмов

Вкладка **Алгоритмы** контрольной панели СКЗИ КриптоПро CSP предназначена для установки различных параметров реализованных в криптопровайдере криптографических алгоритмов.

По умолчанию изменение параметров криптографических алгоритмов через контрольную панель СКЗИ КриптоПро CSP недоступно. Для разблокировки возможности изменения параметров алгоритмов установите значение параметра реестра Windows `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Crypto Pro\Cryptography\CurrentVersion\Parameters\EnableOIDModify` в 1.

Примечание. Для большинства вариантов использования СКЗИ КриптоПро CSP изменение параметров используемых криптографических алгоритмов не требуется. При самостоятельном изменении параметров пользователями корректная работа криптопровайдера не гарантируется.

Для установки параметров криптографических алгоритмов откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Алгоритмы** (см. Рисунок 82).

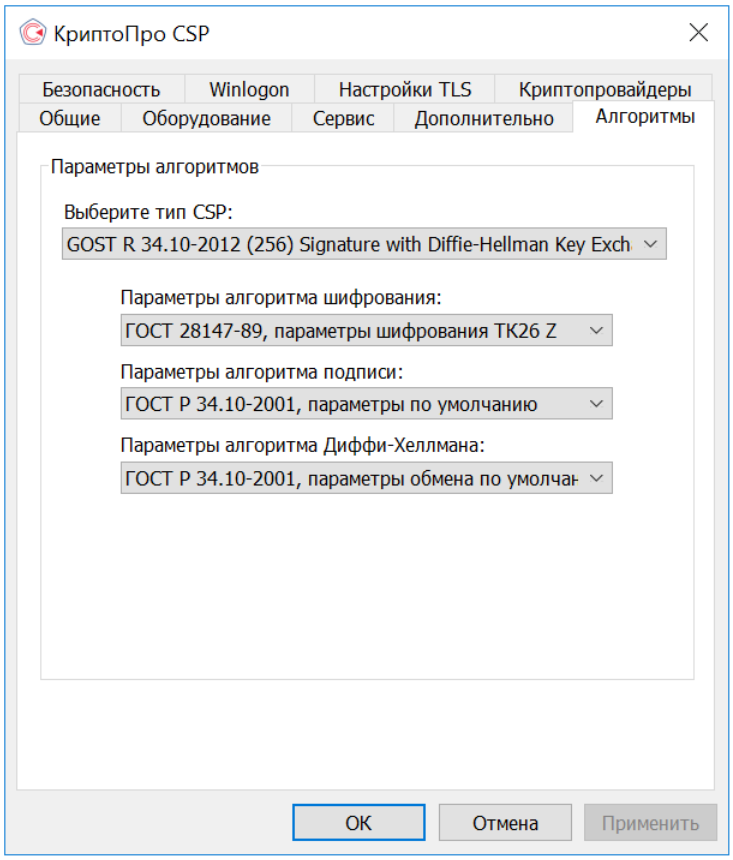


Рисунок 82. Вкладка **Алгоритмы** панели управления

Для установки параметров криптографических алгоритмов на вкладке **Алгоритмы** необходимо выбрать тип криптопровайдера, для которого будет осуществляться настройка. Для соответствующих криптографических алгоритмов реализована возможность установки следующих параметров:

- установка параметров алгоритма шифрования — ГОСТ 28147-89;
- установка параметров алгоритма выработки и проверки электронной цифровой подписи — ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012;
- установка параметров алгоритма Диффи-Хеллмана — ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012.

2.9 Настройка аутентификации в домене Windows

Вкладка **Winlogon** контрольной панели СКЗИ КриптоПро CSP предназначена для настройки аутентификации в домене с использованием алгоритмов ГОСТ.

Для установки параметров аутентификации откройте **Панель управления** СКЗИ КриптоПро CSP и перейдите на вкладку **Winlogon** (см. Рисунок 83).

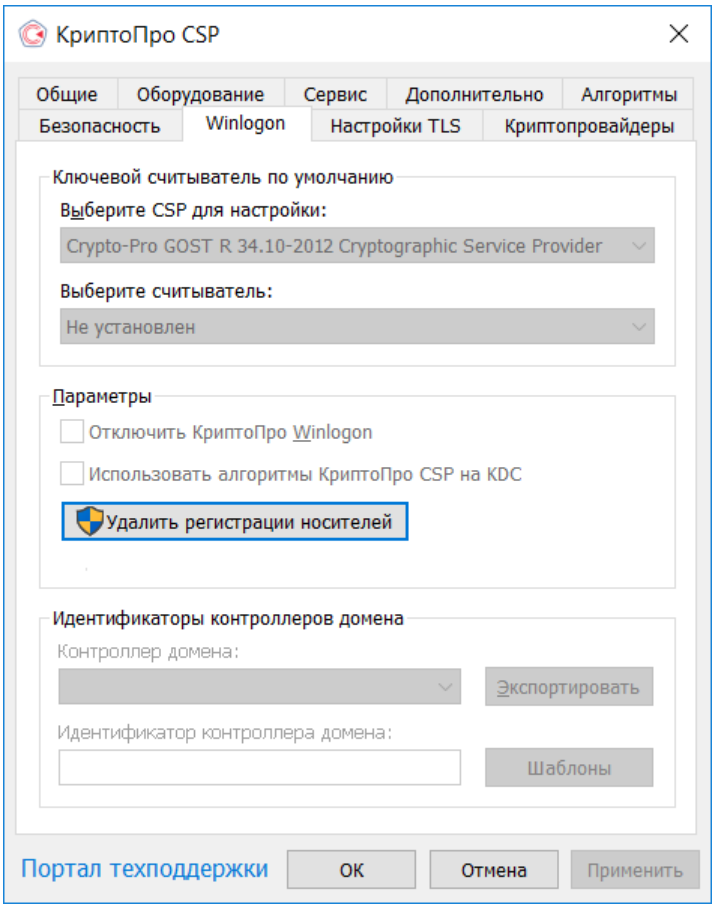


Рисунок 83. Вкладка **Winlogon** панели управления

При установке криптопровайдера на контроллер домена будет доступна для выбора опция **Использовать алгоритмы КриптоПро CSP на KDC** и будут заполнены поля идентификаторов контроллера домена. Подробнее о настройке Winlogon см. разд. 5.

При необходимости можно отключить использование алгоритмов ГОСТ при аутентификации в домене. Для этого предназначена опция **Отключить КриптоПро Winlogon**.

2.10 Настройки TLS

Вкладка **Настройки TLS** контрольной панели СКЗИ КриптоПро CSP предназначена для настройки протокола TLS, обеспечивающего аутентификацию связывающихся сторон, конфиденциальность и целостность пересылаемой информации.

Для установки параметров аутентификации откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Настройки TLS** (см. Рисунок 84).

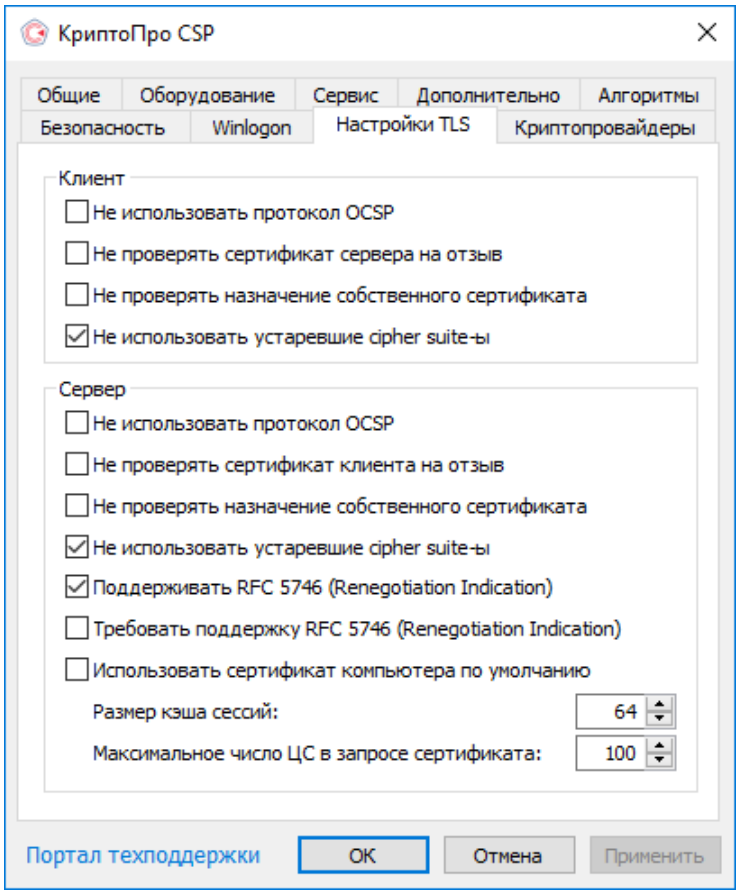


Рисунок 84. Вкладка **Настройки TLS** панели управления

В параметрах Клиента возможна настройка следующих опций:

- **Не использовать протокол OCSP** — отключает возможность использования клиентом протокола проверки сертификата по базе сервера OCSP Responder;
- **Не проверять сертификат сервера на отзыв** — отключает проверку клиентом сертификата сервера на принадлежность списку отозванных сертификатов (CRL);
- **Не проверять назначение собственного сертификата** — отключает проверку назначения собственного сертификата;
- **Не использовать устаревшие cipher suite-ы** — отключает возможность использования cipher suite, в которых были обнаружены уязвимости.

В параметрах Сервера возможна настройка следующих опций:

- **Не использовать протокол OCSP** — отключает возможность использования сервером протокола проверки сертификата по базе сервера OCSP Responder;
- **Не проверять сертификат клиента на отзыв** — отключает проверку сервером сертификата клиента на принадлежность списку отозванных сертификатов (CRL);
- **Не проверять назначение собственного сертификата** — отключает проверку назначения собственного сертификата;
- **Не использовать устаревшие cipher suite-ы** — отключает возможность использования cipher suite, в которых были обнаружены уязвимости;
- **Поддерживать RFC 5746 (Renegotiation Indication)** — включает поддержку сервером расширения Renegotiation Indication протокола TLS (подробнее см. RFC 5746);
- **Требовать поддержку RFC 5746 (Renegotiation Indication)** — включает требование поддержки клиентом расширения Renegotiation Indication протокола TLS (подробнее см. RFC 5746);
- **Использовать сертификат компьютера по умолчанию** — сервером используется сертификат компьютера по умолчанию;
- **Размер кэша сессий** — в поле устанавливается размер кэша сессий;

• **Максимальное число ЦС в запросе сертификата** — в поле устанавливается максимальное число центров сертификации (ЦС) в запросе сертификата.

2.11 Управление криптопровайдерами

Вкладка **Криптопровайдеры** контрольной панели СКЗИ КриптоПро CSP предназначена для назначения криптопровайдеров по умолчанию в случае, если на машине зарегистрировано несколько провайдеров одного типа.

Для назначения криптопровайдеров по умолчанию откройте **Панель управления** СКЗИ КриптоПро CSP. Панель управления должна быть запущена от имени администратора, для этого нажмите на ссылку «Запустить с правами администратора» на вкладке **Общие** (см. Рисунок 18). После перезапуска перейдите на вкладку **Криптопровайдеры** (см. Рисунок 85).

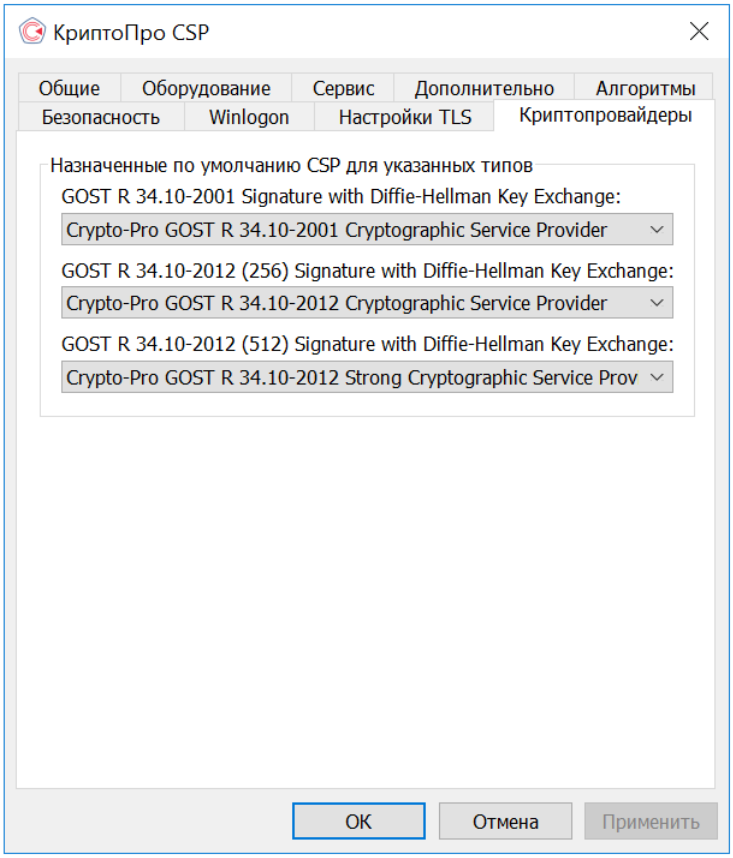


Рисунок 85. Вкладка **Криптопровайдеры** панели управления

3 Интерфейс генерации ключей

КриптоПро CSP может использоваться различными приложениями для создания контейнеров на платформе Windows с использованием службы сертификации Windows Server.

3.1 Генерация ключей и получение сертификата с помощью УЦ

Для формирования личных ключей и получения сертификатов можно воспользоваться Тестовым Удостоверяющим Центром ООО «КРИПТО-ПРО» — https://www.cryptopro.ru/certsrv.

Для формирования запроса сертификата на главной странице тестового УЦ нажмите кнопку **Сформировать ключи и отправить запрос на сертификат** (см. Рисунок 86).

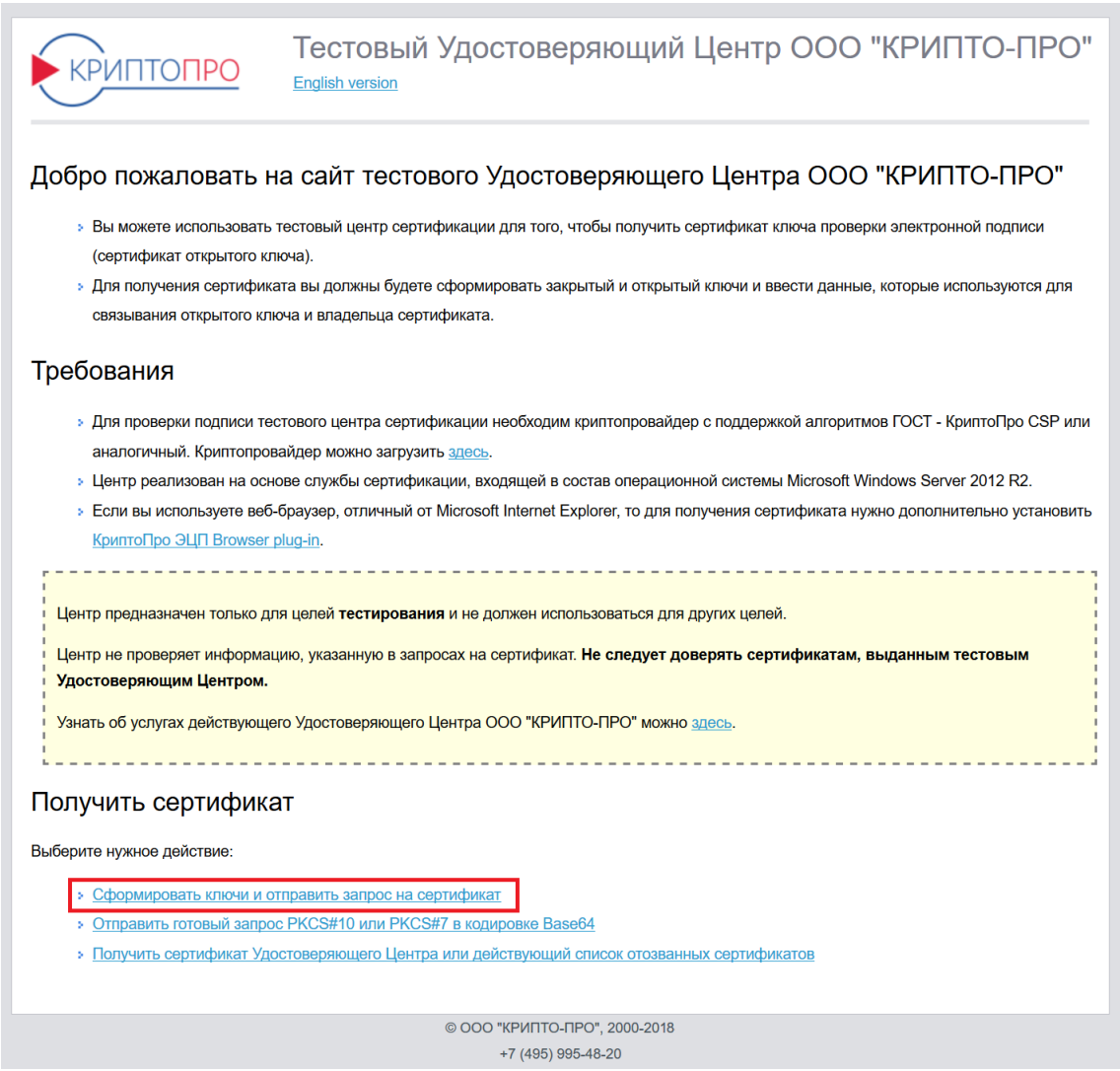


Рисунок 86. Тестовый УЦ ООО «КРИПТО-ПРО»

Откроется форма расширенного запроса сертификата (см. Рисунок 87).

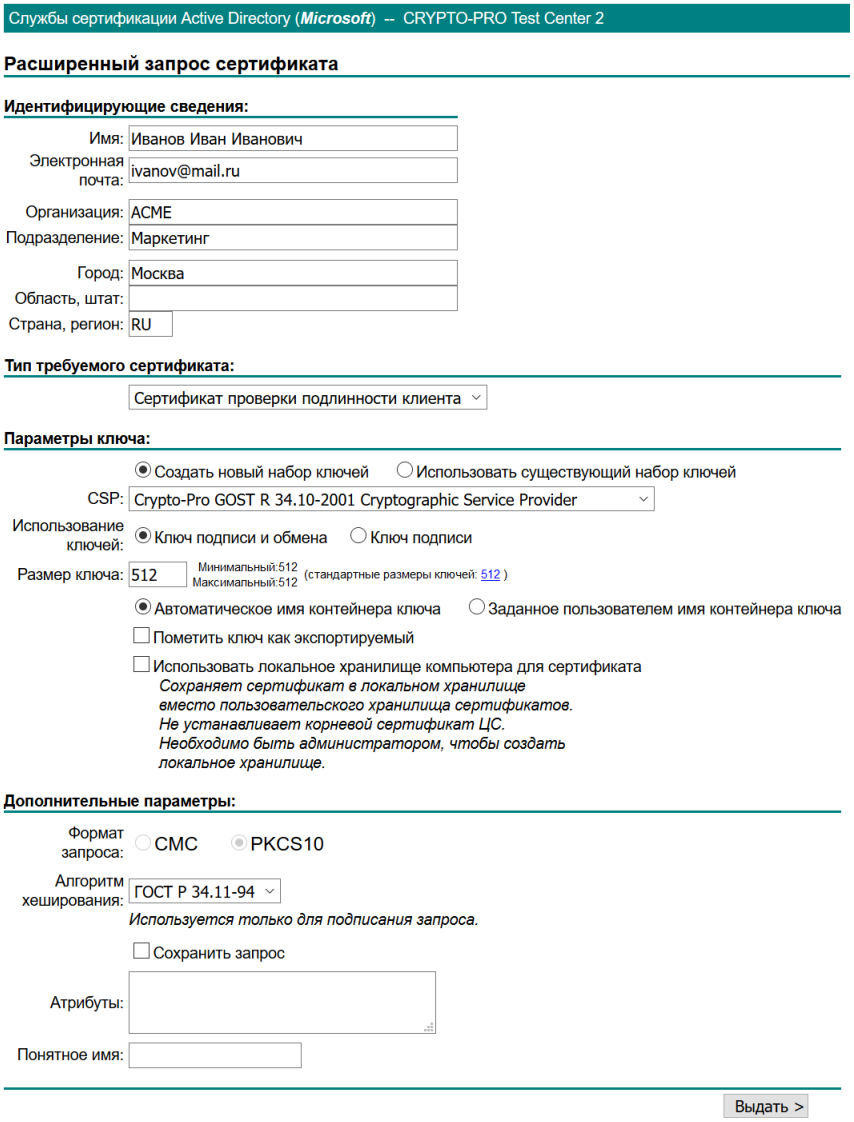


Рисунок 87. Форма расширенного запроса сертификата

В окне формирования запроса на сертификат заполните следующие поля:

- **Имя** — имя владельца сертификата.
- **Электронная почта** — адрес электронной почты. Адрес электронной почты может содержать символы A-Z, a-z, 0-9, некоторые специальные символы, но не может содержать кириллицу.

Примечание. Если введенный адрес электронной почты не совпадает с зарегистрированным адресом в Microsoft Outlook Express (Microsoft Outlook), использовать криптографические функции в электронной почте будет невозможно.

- **Страна, регион** — значение поля страны/региона должно быть представлено в виде двухбуквенного кода по стандарту ISO 3166 (RU для России).
- **Тип требуемого сертификата** — тип сертификата выбирается из выпадающего списка. Если запрашиваемый сертификат предполагается использовать в электронной почте, выберите **Сертификат защиты электронной почты**. Если запрашиваемый сертификат предполагается использовать в протоколе TLS, выберите **Сертификат проверки подлинности клиента**.

Если немедленная установка сертификата не требуется, возможно сохранить запрос сертификата в файле для последующей установки. Для этого установите флаг **Сохранить запрос**. В этом случае сертификат не будет установлен, а результат запроса будет сохранен в виде файла PKCS#10.

После заполнения всех полей нажмите кнопку **Выдать**. Начнется процедура создания запроса и выдачи сертификата.

3.2 Создание ключевого контейнера

3.2.1 Выбор ключевого носителя

При создании ключевого контейнера в случае наличия нескольких устройств, служащих ключевыми носителями, откроется окно выбора ключевого носителя (см. Рисунок 88).

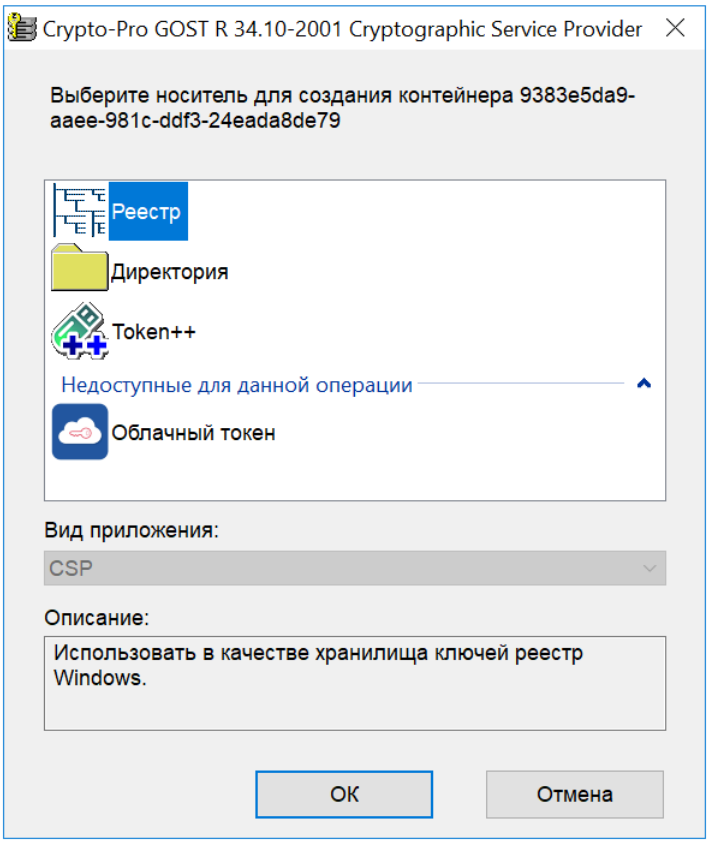


Рисунок 88. Выбор ключевого носителя

При наличии единственного ключевого носителя он автоматически выбирается для хранения контейнера закрытого ключа и данное окно не отображается.

После выбора ключевого носителя нажмите кнопку **OK**.

3.2.2 Генерация начальной последовательности ДСЧ

После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, откроется окно генерации начальной последовательности ДСЧ с помощью биологического ДСЧ (см. Рисунок 89). Для генерации случайной последовательности перемещайте указатель мыши или нажимайте различные клавиши.

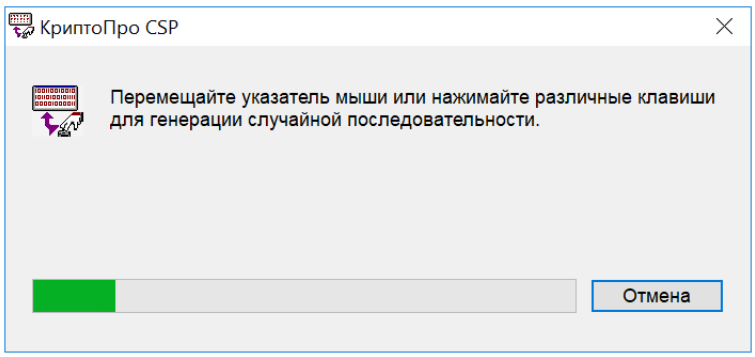


Рисунок 89. Генерация начальной последовательности ДСЧ

3.2.3 Ввод пароля на доступ к закрытому ключу

После завершения работы биологического ДСЧ откроется окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 90).

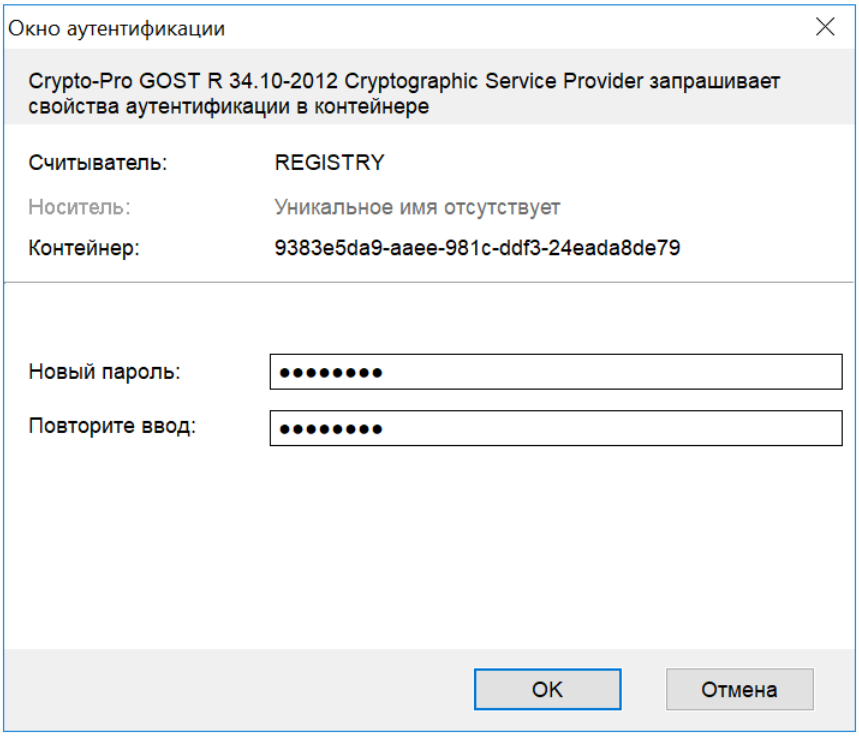


Рисунок 90. Установка пароля на доступ к закрытому ключу

В поле **Новый пароль** введите текстовый пароль на доступ к закрытому ключу создаваемого контейнера и подтвердите его повторным вводом в поле **Повторите ввод**. После ввода пароля нажмите кнопку **OK**.

Если ключ генерируется на носитель, поддерживающий аппаратный пароль или пин-код, то необходимо ввести тот пароль (пин-код), который установлен на этот ключевой носитель. Защита носителей, поддерживающих аппаратный пароль (пин-код), возможна только на этом пароле (пин-коде).

3.2.4 Выбор способа защиты доступа к закрытому ключу

Помимо ввода пароля в СКЗИ КриптоПро CSP существуют другие средства защиты доступа к закрытому ключу. Для выбора подходящего средства защиты на вкладке **Сервис** нажмите кнопку **Изменить пароль** и выберите необходимый контейнер, при необходимости введите пароль на доступ к закрытому ключу (подробнее см. п. 2.5.4.1). Откроется окно выбора способа защиты доступа к закрытому ключу создаваемого контейнера (см. Рисунок 91).

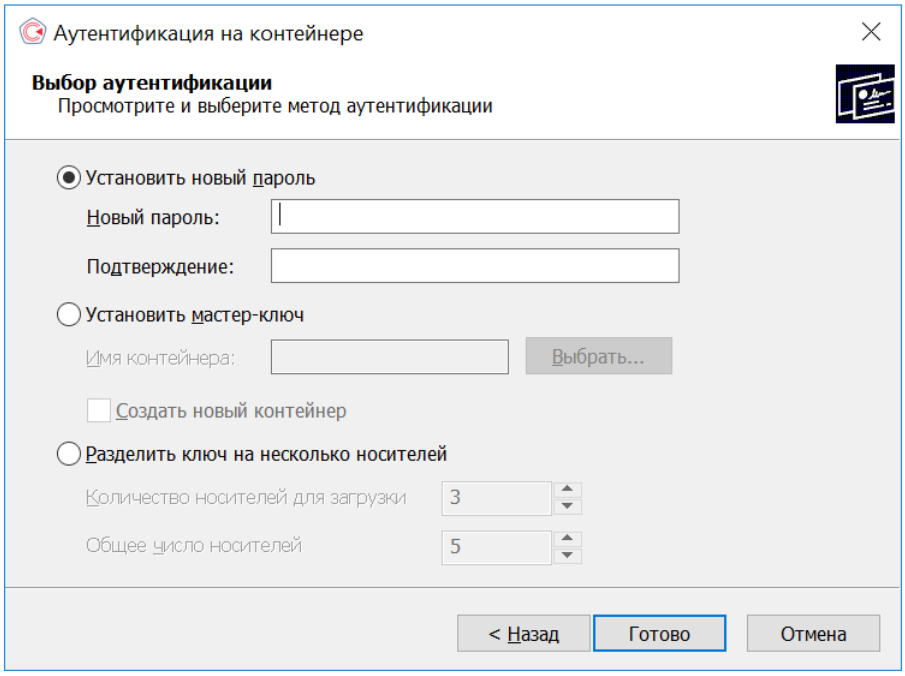


Рисунок 91. Выбор средства защиты доступа к закрытому ключу

В этом окне содержатся следующие поля:

- Установить новый пароль — ввод текстового пароля на доступ к закрытому ключу;
- Установить мастер-ключ — зашифрование данного закрытого ключа на другом закрытом ключе (из другого ключевого контейнера);
- Разделить ключ на несколько носителей — разделение данного закрытого ключа на несколько носителей для обеспечения доступа к нему.

3.2.4.1 Установка нового пароля

Если переключатель установлен в поле **Установить новый пароль**(см. Рисунок 91), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи пароля на доступ, введенного с клавиатуры. Для установки пароля необходимо осуществить действия, описанные в пункте Ввод пароля на доступ к закрытому ключу.

3.2.4.2 Установка мастер-ключа

Если переключатель установлен в поле **Установить мастер-ключ** (см. Рисунок 91), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи зашифрования данного закрытого ключа на другом закрытом ключе.

Для этого необходимо ввести имя контейнера (или выбрать контейнер из списка с помощью кнопки **Выбрать**), содержащего закрытый ключ, на котором будет осуществлено зашифрование исходного закрытого ключа. При нажатии кнопки **Выбрать** откроется список существующих контейнеров (см. Рисунок 92).

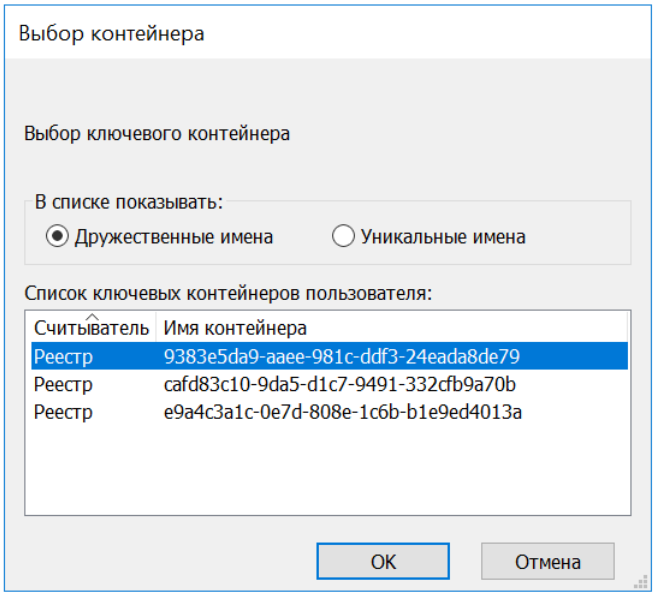


Рисунок 92. Список существующих контейнеров

После выбора необходимого контейнера нажмите кнопку **OK**. При этом произойдет зашифрование данного закрытого ключа на ключе выбранного контейнера. СКЗИ КриптоПро CSP позволяет осуществлять зашифрование данного ключа не только на существующем закрытом ключе. При установке флага напротив поля **Создать новый контейнер** (см. Рисунок 91) будет создан новый контейнер и на его ключе зашифрован закрытый ключ данного контейнера.

3.2.4.3 Разделение ключа на несколько носителей

Если переключатель установлен в поле **Разделить ключ на несколько носителей** (см. Рисунок 91), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи разделения доступа к нему между несколькими ключевыми носителями. Каждый из этих носителей является самостоятельным контейнером с собственным паролем на доступ к закрытому ключу.

В окне заполните следующие поля:

- **Количество носителей для загрузки** — число носителей, необходимых для доступа к закрытому ключу.
- **Общее количество носителей** — общее количество носителей, между которыми ключ будет разделен.

После заполнения этих полей начнётся процесс создания новых контейнеров, участвующих в разделении исходного ключа (количество создаваемых контейнеров равно значению, указанному в поле **Общее количество носителей**):

1) Для каждого создаваемого контейнера откроется окно выбора ключевого носителя (см. Рисунок 88). В этом окне выберите носитель, который будет участвовать в разделении ключа.

2) После того, как для всех контейнеров выбраны носители, откроется окно генерации начальной последовательности ДСЧ (см. Рисунок 89).

3) После завершения генерации начальной последовательности ДСЧ откроется окно ввода пароля на доступ к закрытому ключу для каждого создаваемого контейнера (см. Рисунок 90). В этом окне нужно ввести или выбрать другое средство защиты доступа к закрытому ключу при помощи кнопки **Подробнее** (см. Рисунок 91).

3.3 Установка сертификата в хранилище

После завершения работы биологического ДСЧ и создания контейнера в браузере откроется страница со ссылкой для установки выпущенного сертификата. Для установки сертификата на открывшейся странице нажмите ссылку «Установить этот сертификат» (см. Рисунок 93).

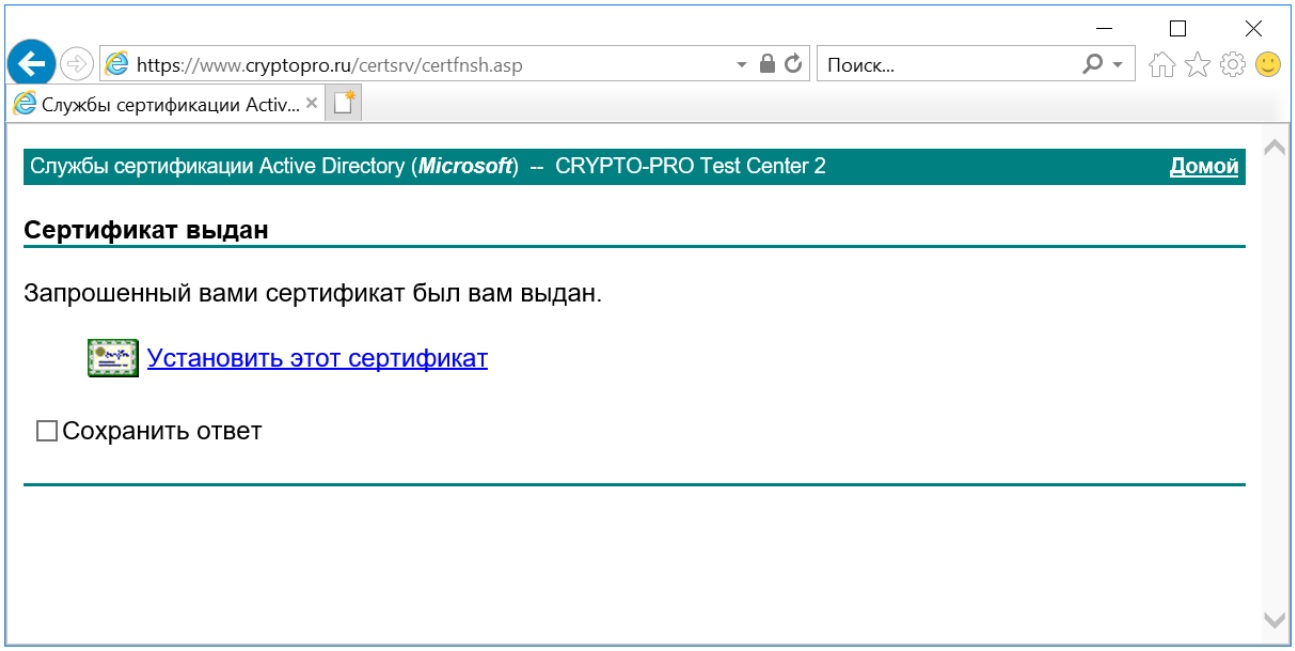


Рисунок 93. Установка сертификата

При установке сертификата в хранилище текущего пользователя запрашивается пароль для контейнера. Введите пароль в окне аутентификации и нажмите кнопку **OK** (см. Рисунок 94).

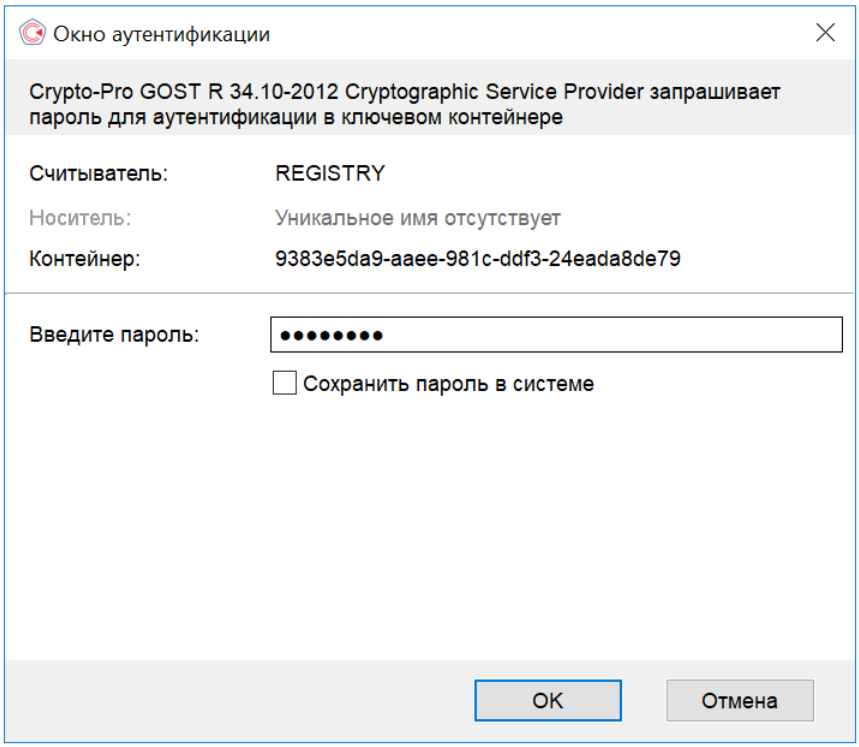


Рисунок 94. Ввод пароля на доступ к контейнеру

При успешной установке сертификата на странице в браузере появится соответствующее сообщение (см. Рисунок 95).

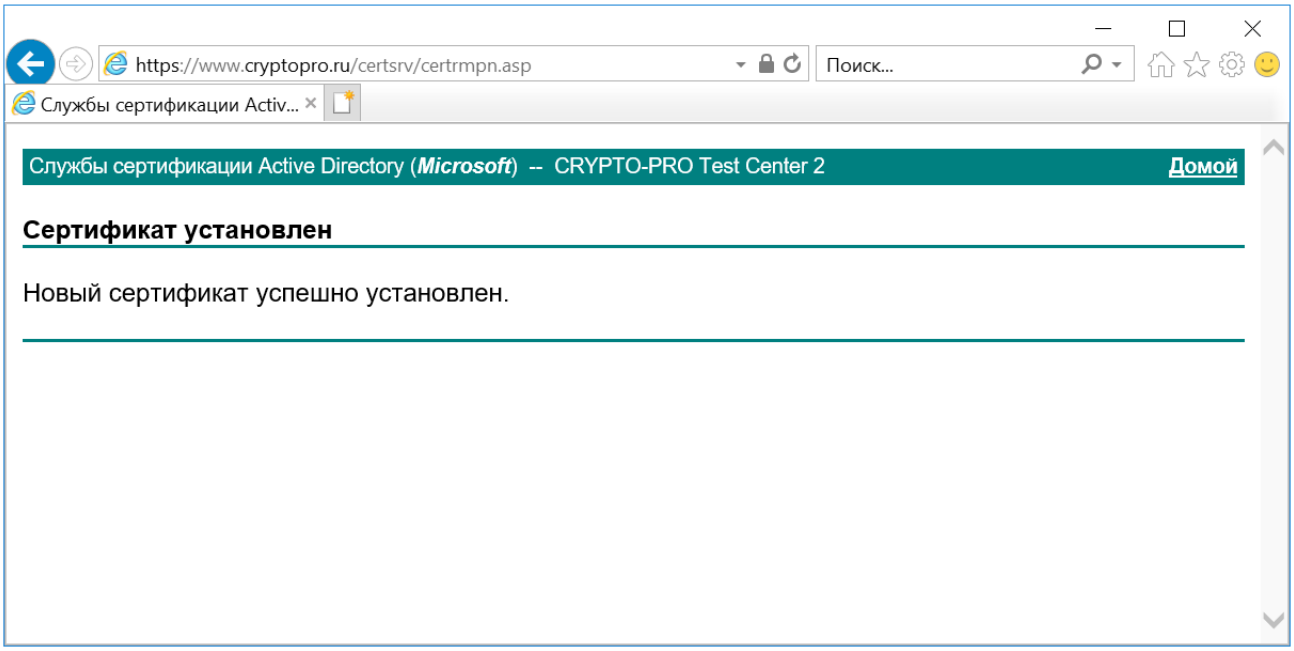


Рисунок 95. Сообщение об успешной установке сертификата

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро. В меню Пуск выберите Все программы ⇒ КРИПТО-ПРО ⇒ Сертификаты. Сертификат должен находиться в хранилище Личное текущего пользователя (см. Рисунок 96).

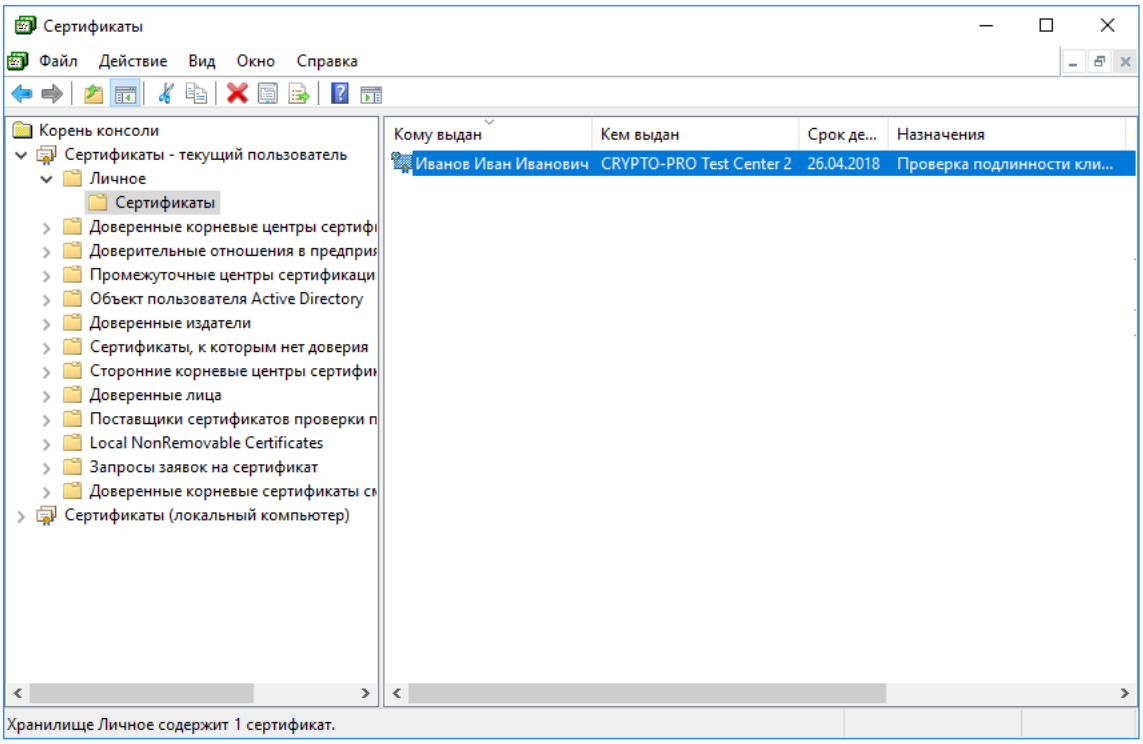


Рисунок 96. Проверка наличия сертификата в хранилище

3.4 Открытие ключевого контейнера

3.4.1 Отсутствие ключевого носителя

В случае отсутствия ключевого носителя при открытии ключевого контейнера появится окно, сообщающее об отсутствии носителя (см. Рисунок 97).

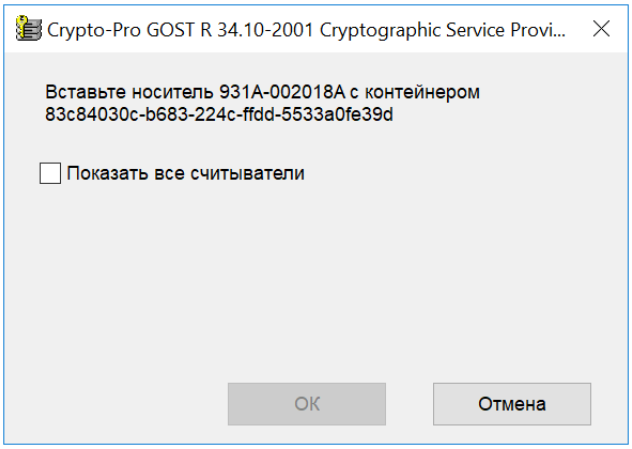


Рисунок 97. Отсутствие необходимого носителя

После того, как носитель будет подключен, откроется окно выбора ключевого носителя (см. Рисунок 98). Укажите носитель для открытия требуемого контейнера и нажмите кнопку **OK**.

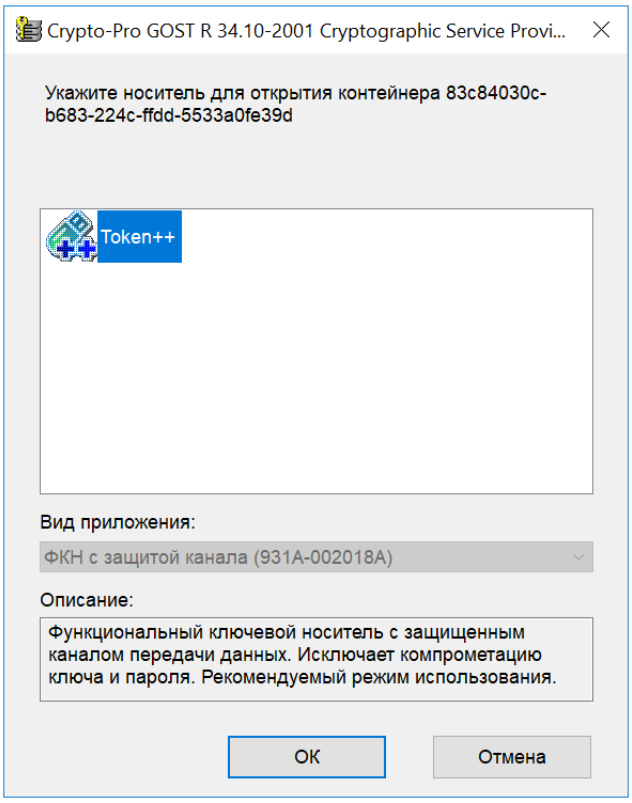


Рисунок 98. Выбор носителя для открытия контейнера

Когда необходимый ключевой носитель подключен, окно, сообщающее об отсутствии ключевого носителя, не отображается.

3.4.2 Проверка пароля на доступ к закрытому ключу

После того, как ключевой носитель установлен, потребуется подтверждение пароля на доступ к закрытому ключу контейнера.

3.4.2.1 Проверка текстового пароля

Если защита доступа к закрытому ключу обеспечена с помощью пароля (см. п. 3.2.4.1), то отображается окно проверки пароля для доступа к закрытому ключу открываемого контейнера (см. Рисунок 99).

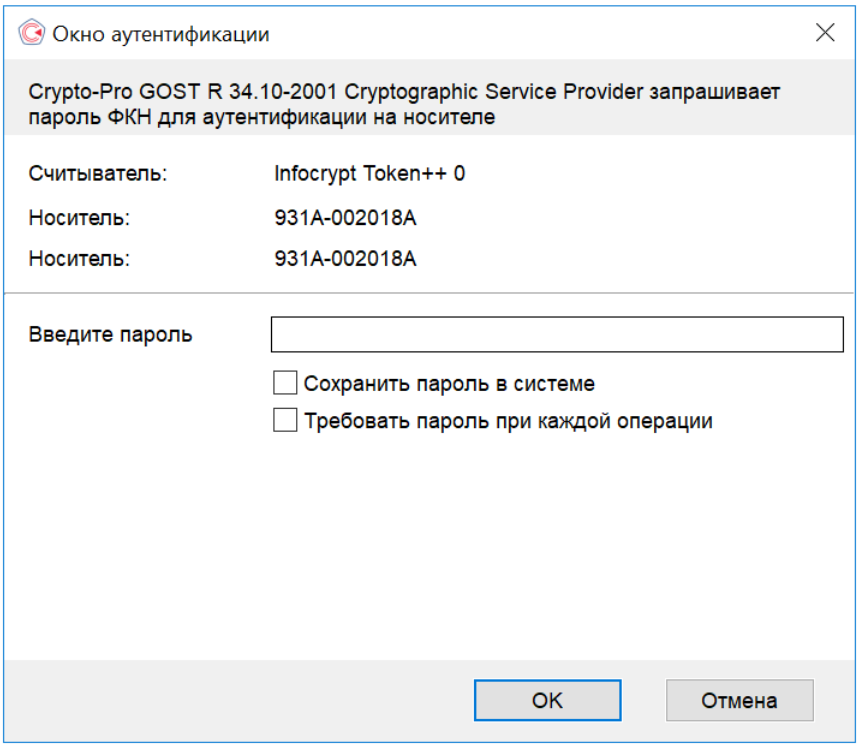


Рисунок 99. Проверка пароля на доступ к закрытому ключу

Если ранее во время ввода пароля на доступ к закрытому ключу флаг напротив поля **Сохранить пароль** был установлен, то пароль был сохранен в реестре. Повторный ввод (проверка) этого пароля не требуется, поэтому окно проверки пароля отображено не будет.

Если пароль введен неверно, будет предложено повторно ввести пароль.

Примечание. Носители, имеющие аппаратный пин-код, могут иметь ограничение на количество неудачных попыток ввода пароля. Превышение этого предела приводит к блокированию носителя или контейнера.

3.4.2.2 Проверка пароля при зашифровании ключа на другом ключе

Если защита доступа к закрытому ключу обеспечена при помощи зашифрования данного закрытого ключа на другом закрытом ключе (см. пункт 3.2.4.2), то будет отображено окно проверки пароля для доступа к закрытому ключу контейнера, на ключе которого проводилось зашифрование (см. Рисунок 99).

После того, как был получен доступ к ключу расшифрования, произойдет расшифрование ключа открываемого контейнера.

3.4.2.3 Проверка пароля при разделении ключа между несколькими носителями

Если защита доступа к закрытому ключу обеспечена при помощи разделения ключа между носителями (см. пункт 3.2.4.3), то проверку требуется осуществить для такого количества носителей, какое было указано в поле **Количество**

носителей для загрузки при создании контейнера (см. Рисунок 91). При обнаружении одного из ключей будет произведена стандартная проверка пароля для ключа-части.

При открытии одного из носителей, участвующего в разделении ключа некоторого контейнера (а все они в свою очередь также являются носителями), проверка пароля на доступ к закрытому ключу проводится в соответствии со способом защиты доступа к ключу, примененным к данному носителю. В общем случае, для разных носителей, участвующих в разделении закрытого ключа одного и того же контейнера, могут быть применены разные способы защиты доступа к ключу.

4 Описание использования, настроек и управления ключами модуля сетевой аутентификации КриптоПро TLS

Для настройки двустороннего соединения (клиент-сервер) по протоколу TLS пользователю с правами администратора необходимо выполнить следующие действия:

1) Установить IIS;
2) Установить КриптоПро CSP;
3) Установить корневой сертификат в хранилище компьютера;
4) Установить сертификат в IIS и настроить двустороннюю аутентификацию;
5) Установить сертификат пользователя;
6) Выполнить проверку соединения.

Примечание. При необходимости обеспечения доступа к веб-серверу по TLS со стороны клиентов, использующих различные браузеры, часть из которых имеет поддержку ГОСТ TLS, а часть — нет, можно настроить IIS на сервере на одновременное использование сертификатов ГОСТ и RSA, см. разд. 4.7.

С целью демонстрации работы криптопровайдера для выпуска тестовых сертификатов используется Тестовый УЦ на сайте https://www.cryptopro.ru/certsrv.

4.1 Установка IIS на сервере

Если службы IIS не установлены в операционной системе Windows используемой версии по умолчанию, необходимо выполнить их установку с помощью пользовательского интерфейса через Компоненты Windows.

Для этого откройте меню Пуск ⇒ Панель управления ⇒ Программы ⇒ Программы и компоненты ⇒ Включение и отключение компонентов Windows. В диалоговом окне Компоненты Windows выберите службы IIS. Для работы по TLS обязательно должны быть указаны службы интернета и средства управления веб-сайтом (см. Рисунок 100). Нажмите кнопку **OK** для выполнения настройки сервера.

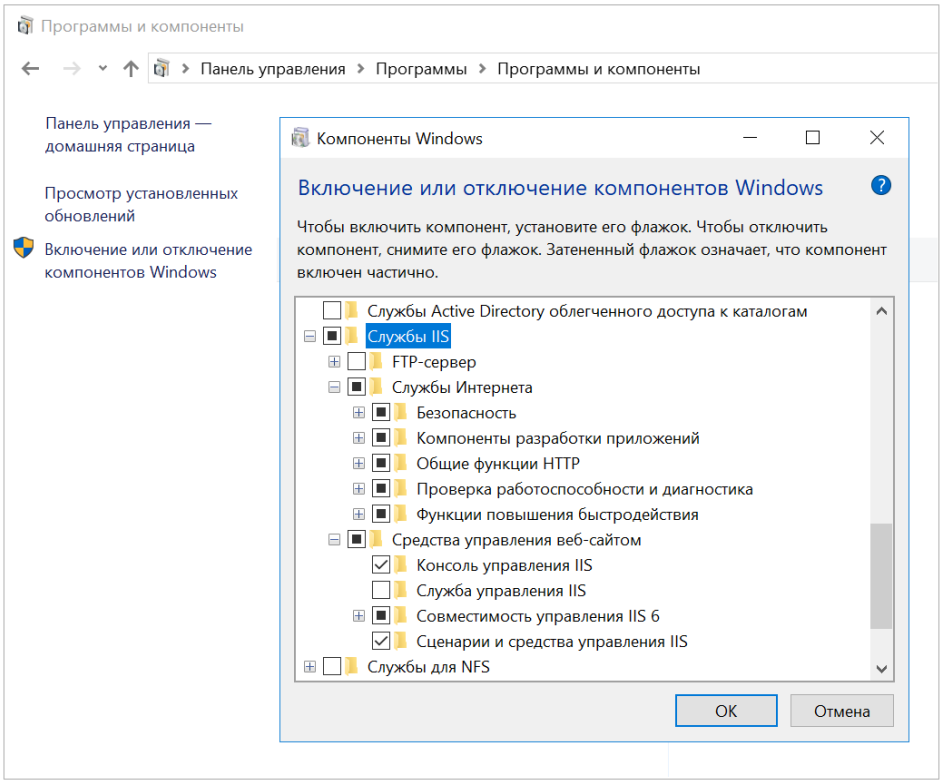


Рисунок 100. Включение компонентов IIS

4.2 Установка КриптоПро CSP

Установка КриптоПро CSP выполняется запуском файла CSPSetup.exe, далее пошагово с помощью мастера установки (см. раздел Инсталляция СКЗИ КриптоПро CSP). При выборе вида установки укажите Выборочную установку, чтобы иметь возможность включить компоненты, не входящие в стандартный набор по умолчанию.

В диалоге выборочной установки необходимо указать, что приложение будет использовано в качестве криптопровайдера уровня ядра ОС (см. Рисунок 101).

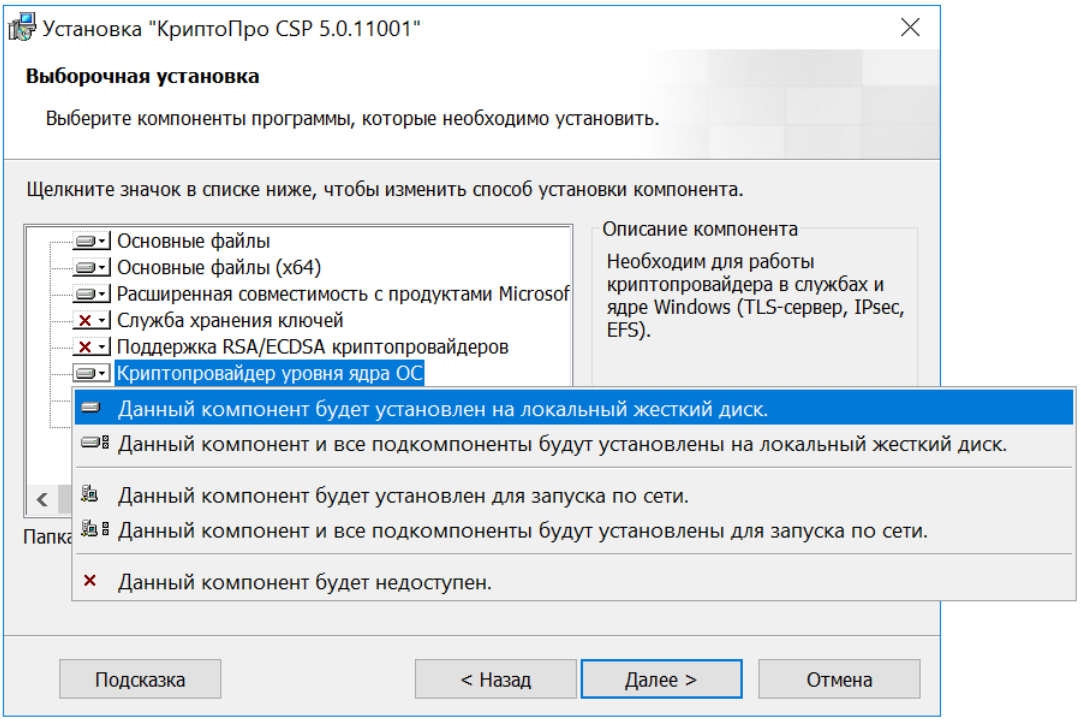


Рисунок 101. Включение компонентов КриптоПро CSP при установке

Далее установка производится с рекомендуемыми по умолчанию параметрами. По завершении установки перезагрузите компьютер.

Для того, чтобы ввести лицензию на TLS или проверить её наличие, воспользуйтесь оснасткой **Управление лицензиями КриптоПро PKI**, которая открывается через меню Пуск (Все программы ⇒ КРИПТО-ПРО ⇒ Управление лицензиями КриптоПро PKI).

4.3 Установка корневого сертификата в хранилище компьютера

Для корректной работы сервера в хранилище сертификатов должен быть установлен сертификат корневого удостоверяющего центра. Для получения сертификата используется Тестовый УЦ КриптоПро.

Браузер, через который осуществляется доступ к веб-интерфейсу центра сертификации, нужно открыть от имени администратора. Откройте веб-интерфейс центра сертификации КриптоПро https://www.cryptopro.ru/certsrv.

Для корректной работы с функционалом выпуска сертификатов необходимо добавить адрес центра сертификации в доверенные сайты в настройках браузера. Для этого в свойствах браузера выберите вкладку Безопасность, в список надежных сайтов добавьте узел https://www.cryptopro.ru/ и сохраните изменения свойств.

На странице Тестового УЦ из списка действий выберите **Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов** (см. Рисунок 102). Корневой сертификат необходимо получать доверенным образом.

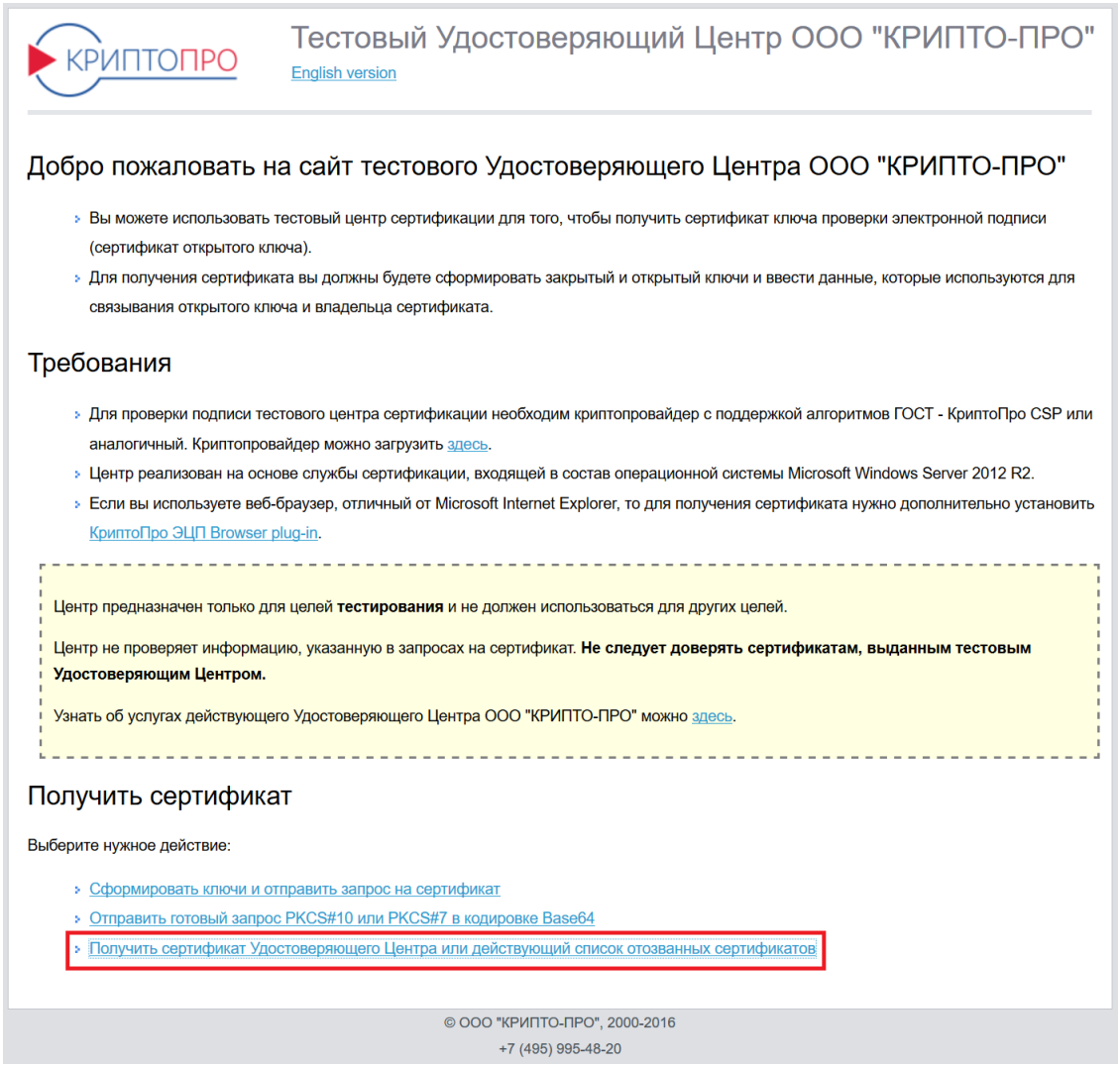


Рисунок 102. Тестовый УЦ КриптоПро

Далее выполняется загрузка сертификата центра сертификации. Выберите метод шифрования и нажмите на ссылку **Загрузка сертификата ЦС** (см. Рисунок 103).

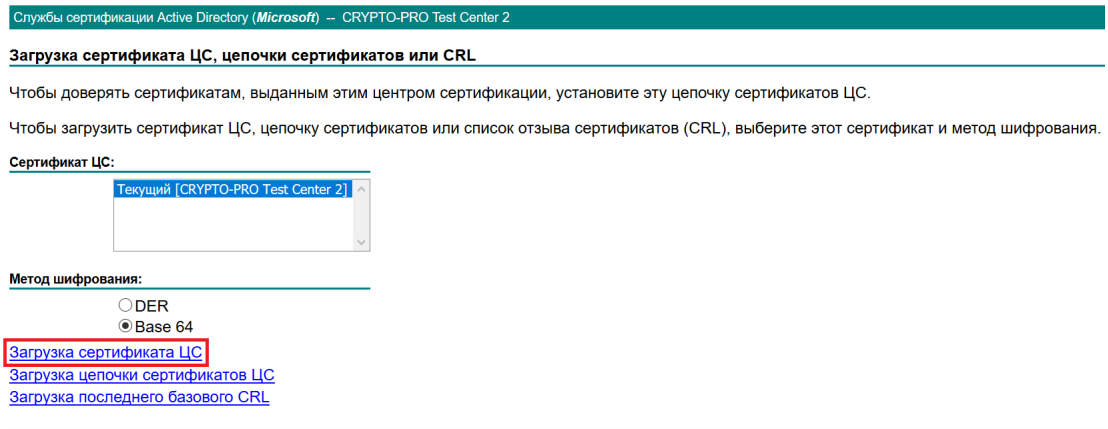


Рисунок 103. Загрузка сертификата ЦС

При получении сертификата необходимо выбрать опцию **Открыть сертификат**. Если данный сертификат ранее

не был установлен в хранилище доверенных корневых центров сертификации, его необходимо установить. Для этого в окне просмотра сведений о сертификате нажмите кнопку **Установить сертификат** (см. Рисунок 104).

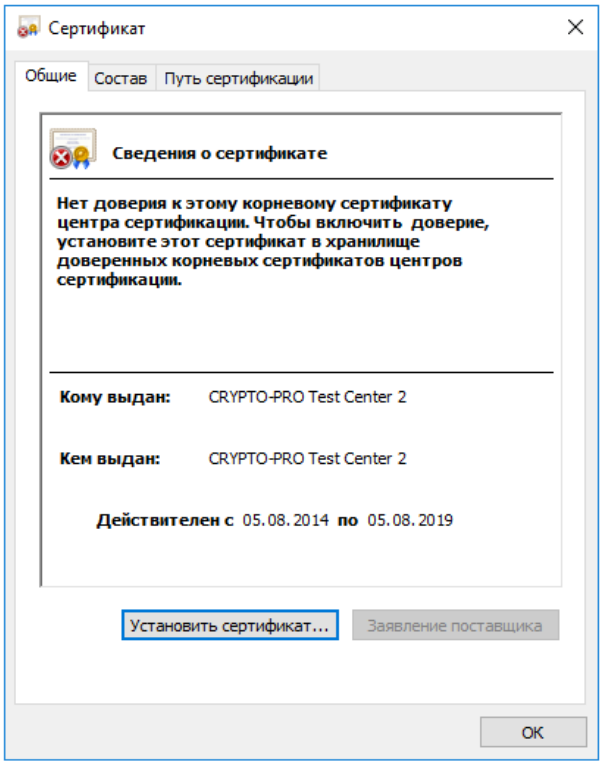


Рисунок 104. Просмотр сертификата ЦС

Откроется Мастер импорта сертификатов. В окне выбора расположения хранилища сертификатов выберите **Локальный компьютер** и нажмите кнопку **Далее**. В следующем окне выбора хранилища сертификатов укажите **Поместить сертификаты в следующее хранилище** и укажите хранилище «Доверенных корневые центры сертификации» (см. Рисунок 105).

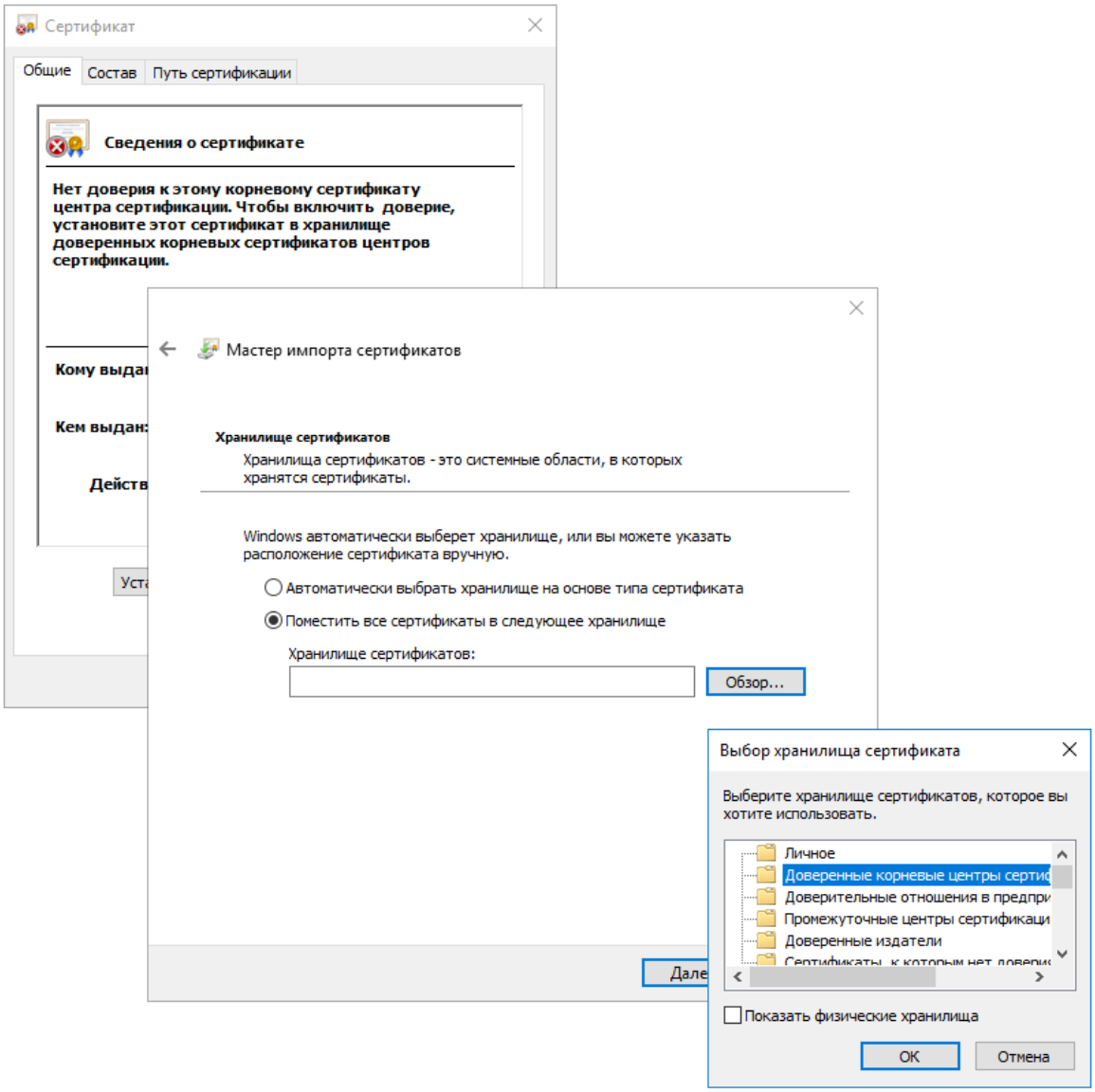


Рисунок 105. Установка сертификата ЦС

Завершите установку сертификата, следуя дальнейшим указаниям мастера.

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро CSP. В меню Пуск выберите Все программы ⇒ КРИПТО-ПРО ⇒ Сертификаты.

Правильно установленный корневой сертификат должен располагаться в хранилище «Доверенные корневые центры сертификации» локального компьютера (см. Рисунок 106).

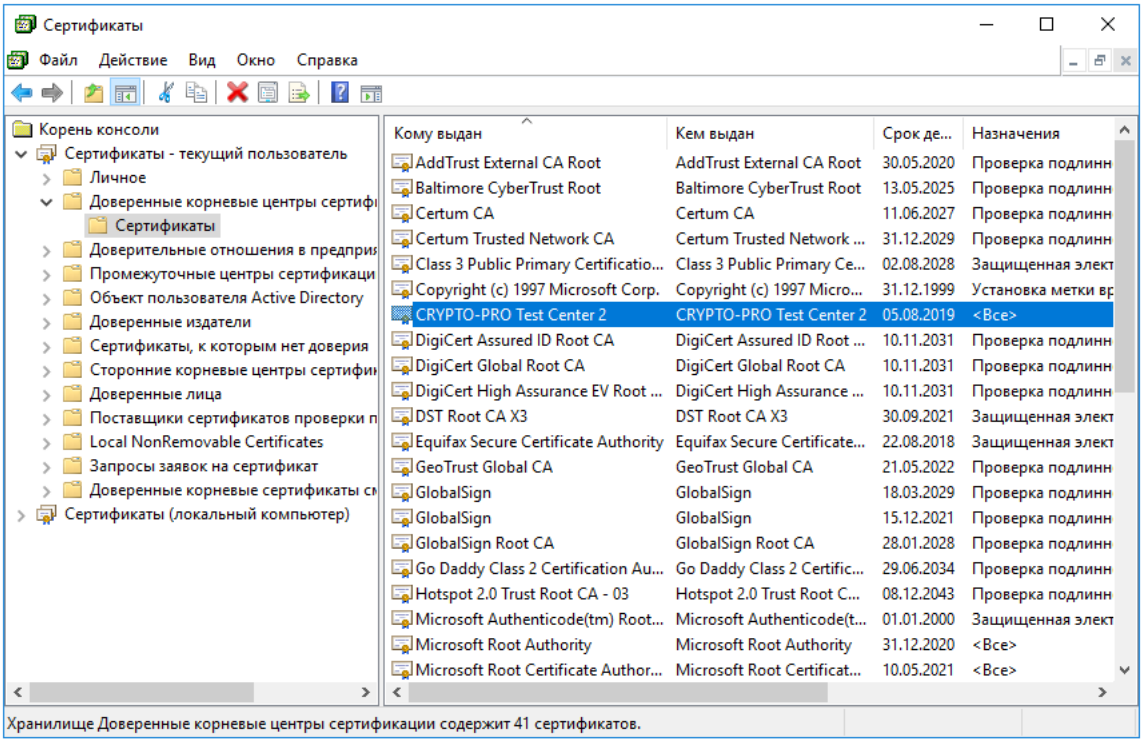


Рисунок 106. Хранилище Доверенные корневые центры сертификации

4.4 Установка сертификата IIS

Для настройки соединения с сервером по протоколу TLS необходимо выполнить следующие действия:
1) выпустить сертификат IIS, если он не был выпущен ранее, и установить его в соответствующее хранилище;
2) настроить IIS с указанием сертификата;
3) проверить соединение по HTTPS.

4.4.1 Выпуск сертификата IIS

Для получения сертификата используется Тестовый УЦ КриптоПро.

Браузер, через который осуществляется доступ к веб-интерфейсу центра сертификации, нужно открыть от имени администратора.

Для выпуска и установки сертификата IIS выполните действия, указанные в разд. 3, с учетом приведенных ниже рекомендаций.

Рекомендации по выпуску и установке сертификата IIS:
- В поле **Имя** укажите имя сертификата. Оно должно совпадать с наименованием домена, обслуживаемого сервером IIS, для которого выпускается сертификат.
- В поле **Тип сертификата** укажите «Сертификат проверки подлинности сервера».
- В секции **Параметры ключа** укажите «Использовать новый набор ключей» и выберите CSP.
- Если в дальнейшем предполагаются манипуляции с ключом сертификата, установите флаг «Пометить ключ как экспортируемый» и в дополнительных параметрах укажите понятное имя.
- Остальные параметры запроса оставьте по умолчанию.
- Не устанавливайте пароль на доступ к закрытому ключу создаваемого контейнера. Для этого оставьте пустыми поля в окне ввода пароля и нажмите кнопку **OK** (см. п. 3.2.4.1).

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро. В меню Пуск выберите Все программы ⇒ КРИПТО-ПРО ⇒ Сертификаты. Сертификат службы IIS должен находиться в хранилище Личное локального компьютера (см. Рисунок 107).

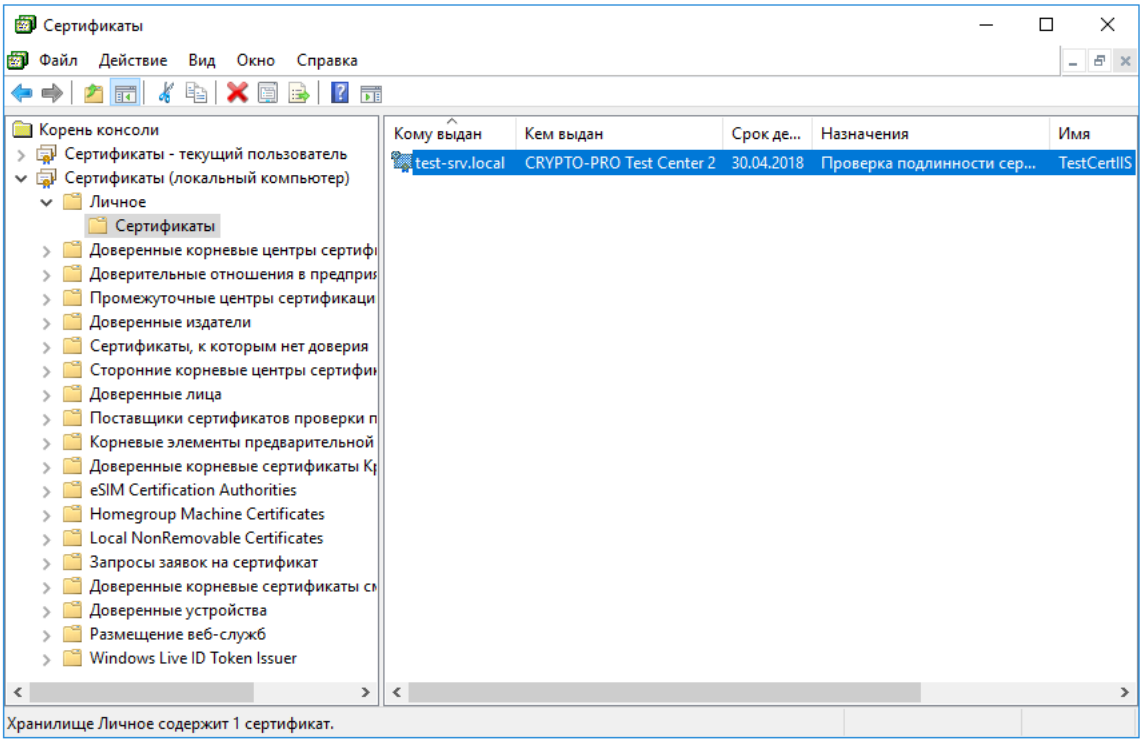


Рисунок 107. Проверка наличия сертификата IIS в хранилище локального компьютера

Если сертификат не попал в хранилище Личное локального компьютера, то найдите его в хранилище текущего пользователя через оснастку **Сертификаты** и перенесите в указанное хранилище.

4.4.2 Настройка IIS с указанием сертификата

Для настройки IIS откройте диспетчер служб IIS одним из следующих способов:
- откройте Панель управления ⇒ Администрирование ⇒ Диспетчер служб IIS;
- вызовите командную строку комбинацией клавиш Win+R и введите команду `inetmgr`.

В Диспетчере служб IIS щелкните правой кнопкой мыши на Веб-узел по-умолчанию (Default Web Site) и выберите в контекстном меню Изменить привязки... (Edit Bindings...) (см. Рисунок 108).

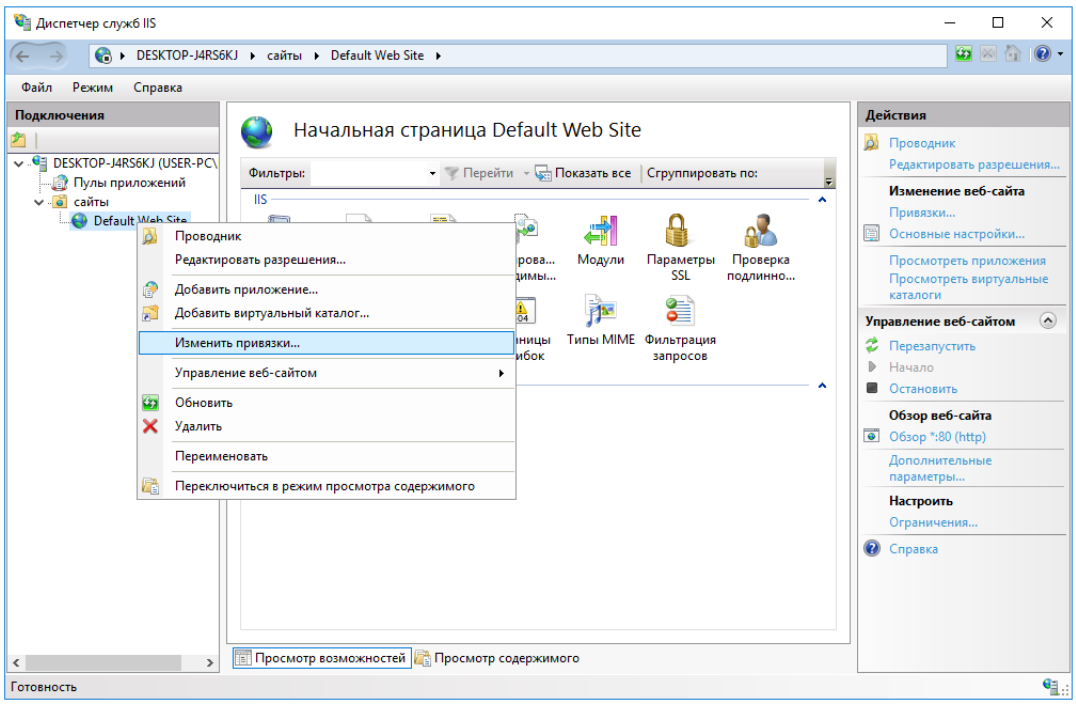


Рисунок 108. Диспетчер IIS

Откроется окно «Привязки сайта». В списке привязок сайта нажмите кнопку **Добавить...** (**Add...**). (см. Рисунок 109).

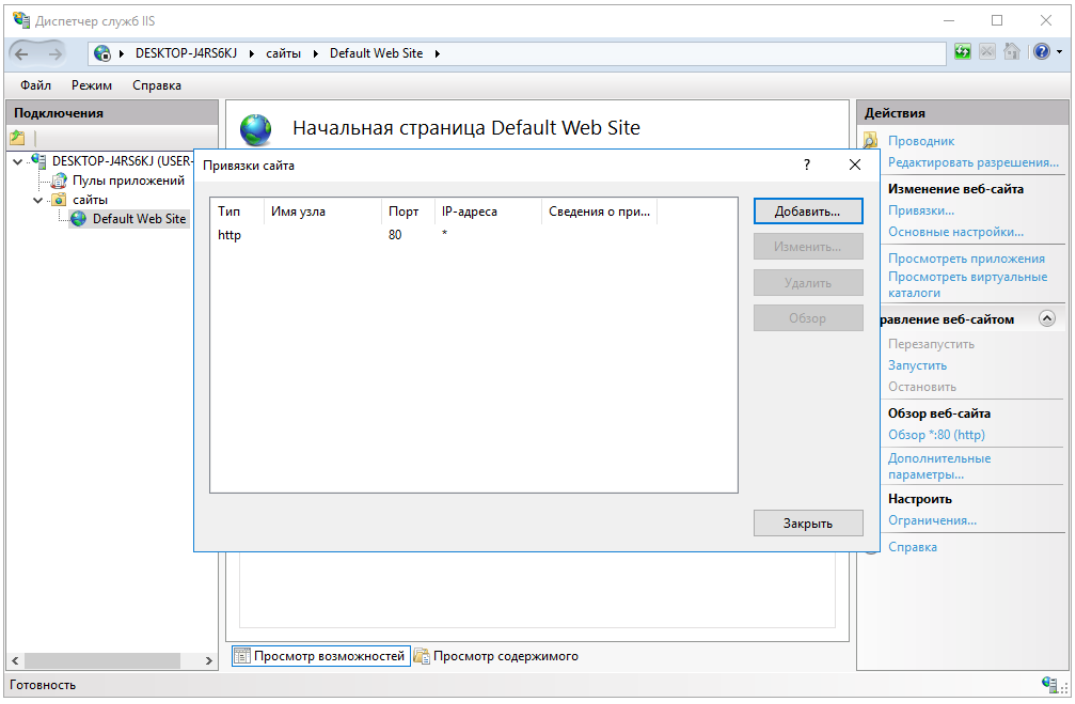


Рисунок 109. Привязки сайта

В открывшемся диалоге добавления привязки сайта (см. Рисунок 110) укажите тип протокола подключения (Type) HTTPS, а в выпадающем списке Сертификаты SSL (SSL certificate) выберите сертификат, созданный для служб IIS. Нажмите кнопку **OK** для сохранения параметров.

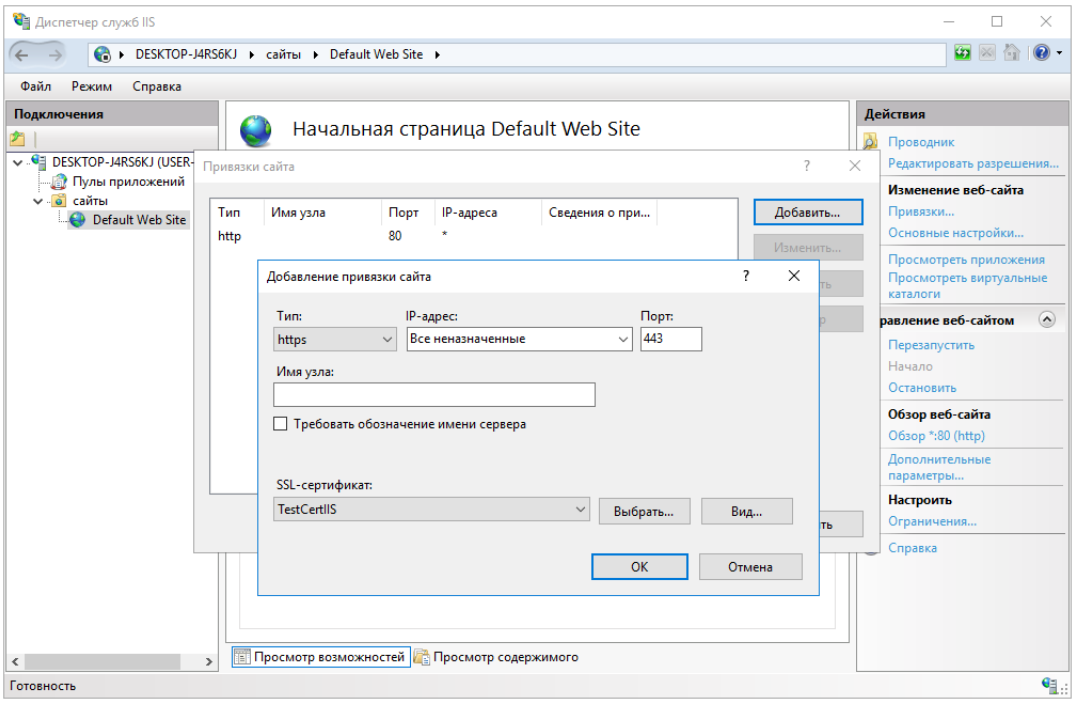


Рисунок 110. Добавление сертификата SSL

Закройте окно «Привязки сайта» и перезапустите IIS, нажав кнопку **Перезапустить** (**Restart**) в окне диспетчера (см. Рисунок 111).

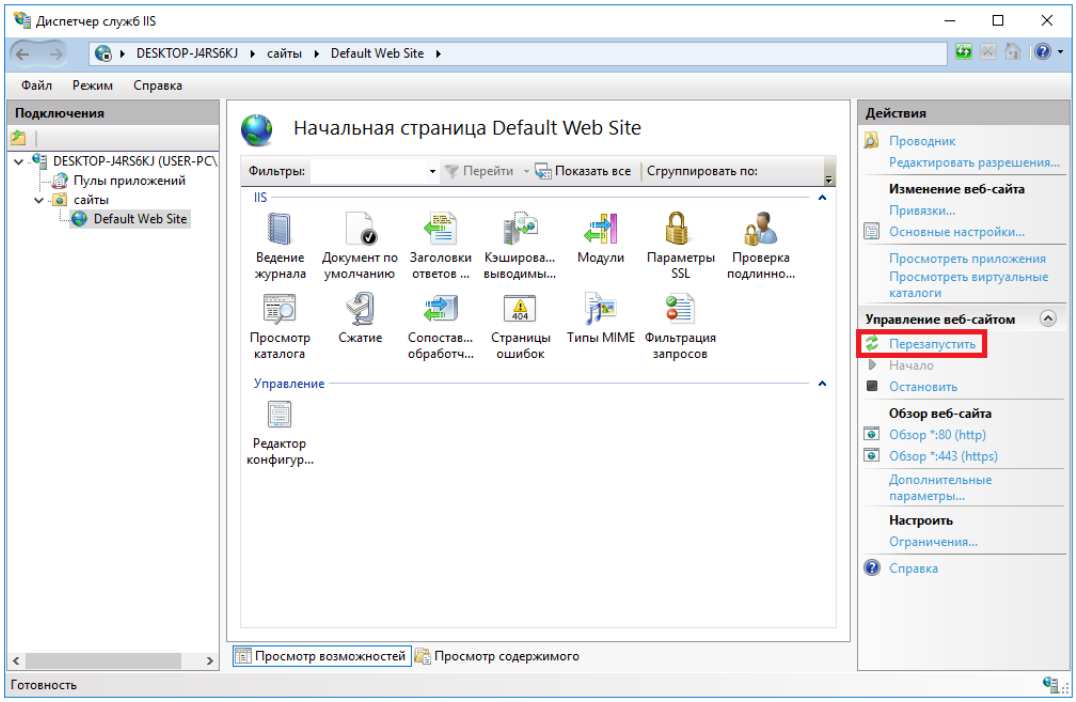


Рисунок 111. Перезапуск IIS

4.4.3 Проверка соединения по HTTPS

Для локальной проверки соединения используйте ссылку **Browse *:443 (https)** в левой части окна менеджера IIS (см. Рисунок 112) или с помощью браузера откройте ссылку https://<domainname>/, где <domainname> – доменное имя настраиваемого сайта (где предварительно должен быть настроен DNS).

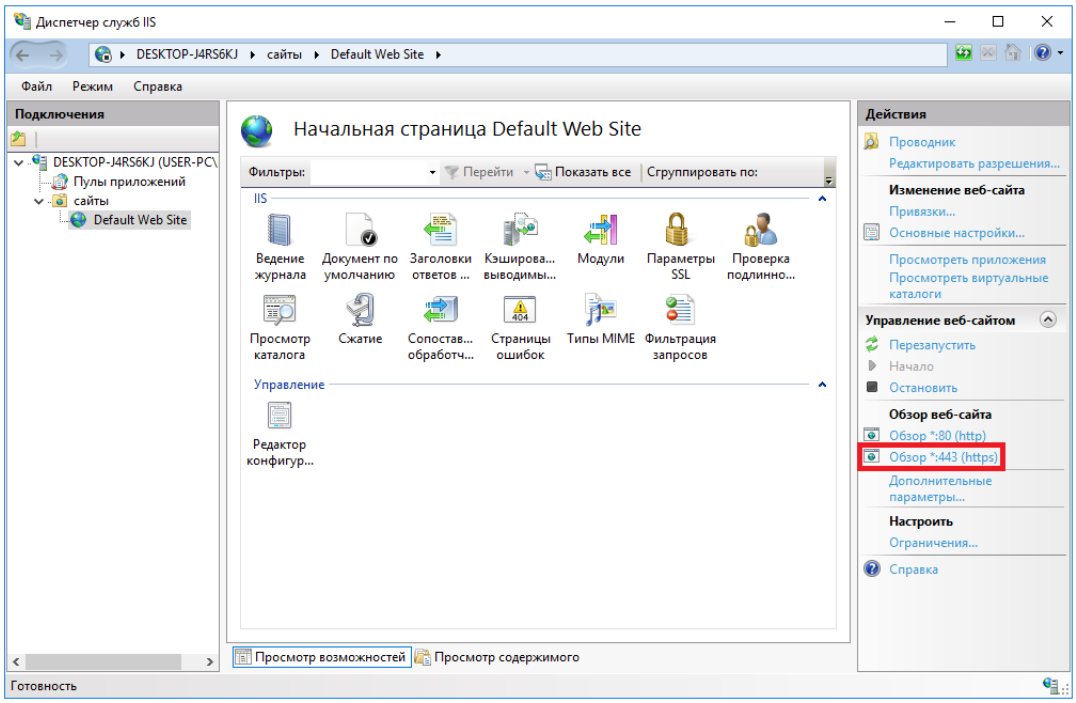


Рисунок 112. Проверка соединения с сервером по HTTPS

СКЗИ КриптоПро CSP, функционирующее в ОС Windows 10, также поддерживает работу в рамках HTTP/2 при взаимодействии с Internet Explorer/Edge и Internet Information Services (IIS). Для обратной совместимости с протоколом HTTP в случае возникновения проблем, связанных с отсутствием поддержки HTTP/2 на клиенте/сервере, необходимо в настройках Internet Explorer/Edge/IIS отключить поддержку HTTP/2 (на сервере отключается параметром `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\EnableHttp2Tls REG_DWORD 0`).

Если службы IIS настроены правильно, в браузере отобразится соответствующая страница (см. Рисунок 113).

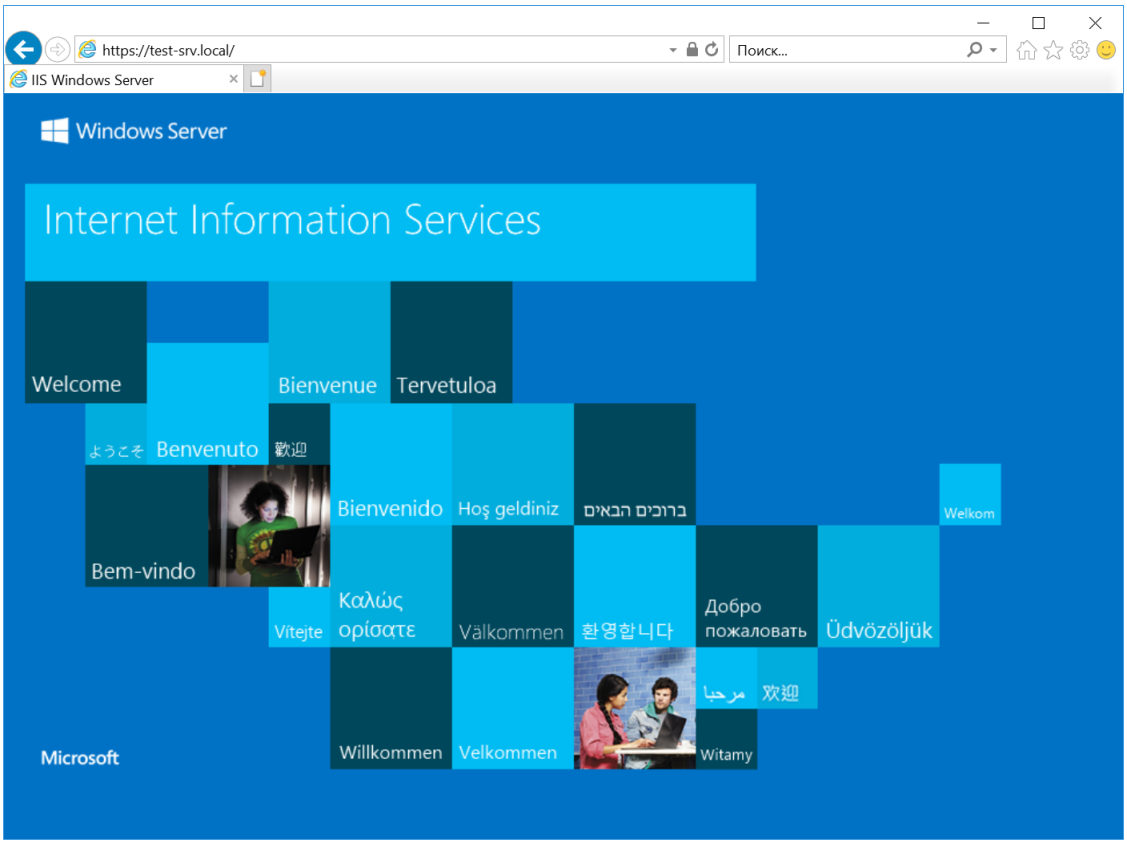


Рисунок 113. Результат проверки соединения с сервером по HTTPS

Для того, чтобы сервер IIS поддерживал двустороннюю аутентификацию с браузером пользователя, нужно выставить в параметрах IIS соответствующие требования. Для этого в Диспетчере служб IIS выделите Веб-узел по-умолчанию (Default Web Site) и выберите в открывшемся меню Параметры SSL (SSL settings) (см. Рисунок 114).

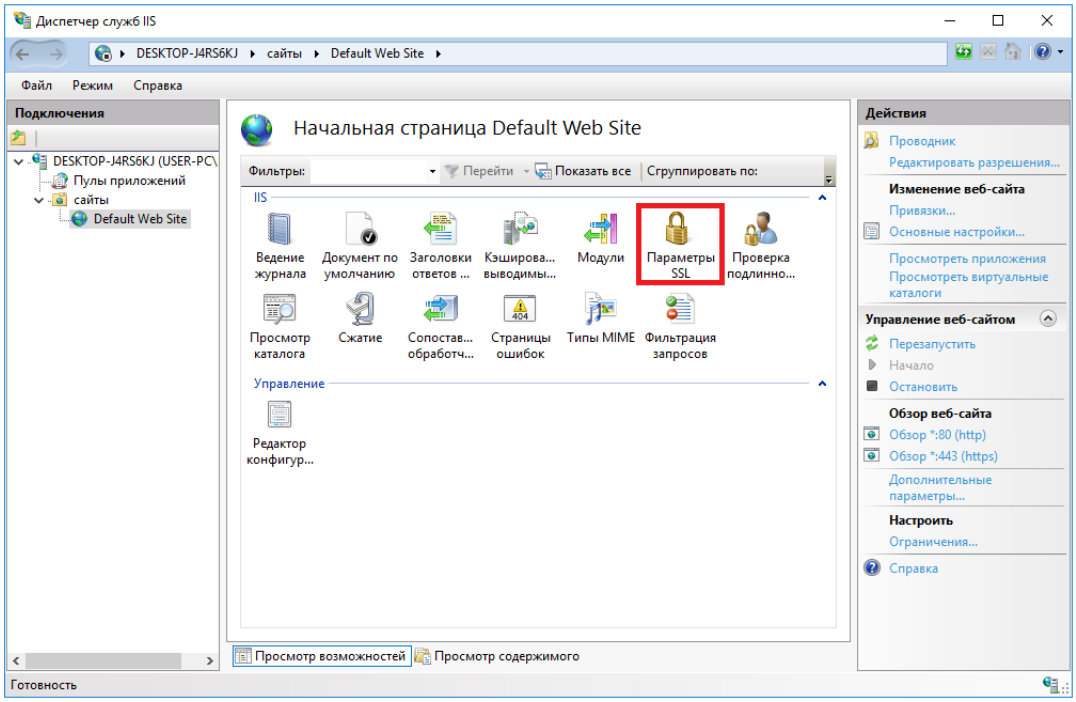


Рисунок 114. Настройка двусторонней аутентификации

В окне настройки параметров SSL установите флаг «Требовать SSL» (Require SSL) и укажите для сертификатов клиента «Требовать» (Require) (см. Рисунок 115). После этого нажмите кнопку **Применить** (**Apply**) для сохранения изменений и перезапустите IIS описанным выше способом (см. Рисунок 111).

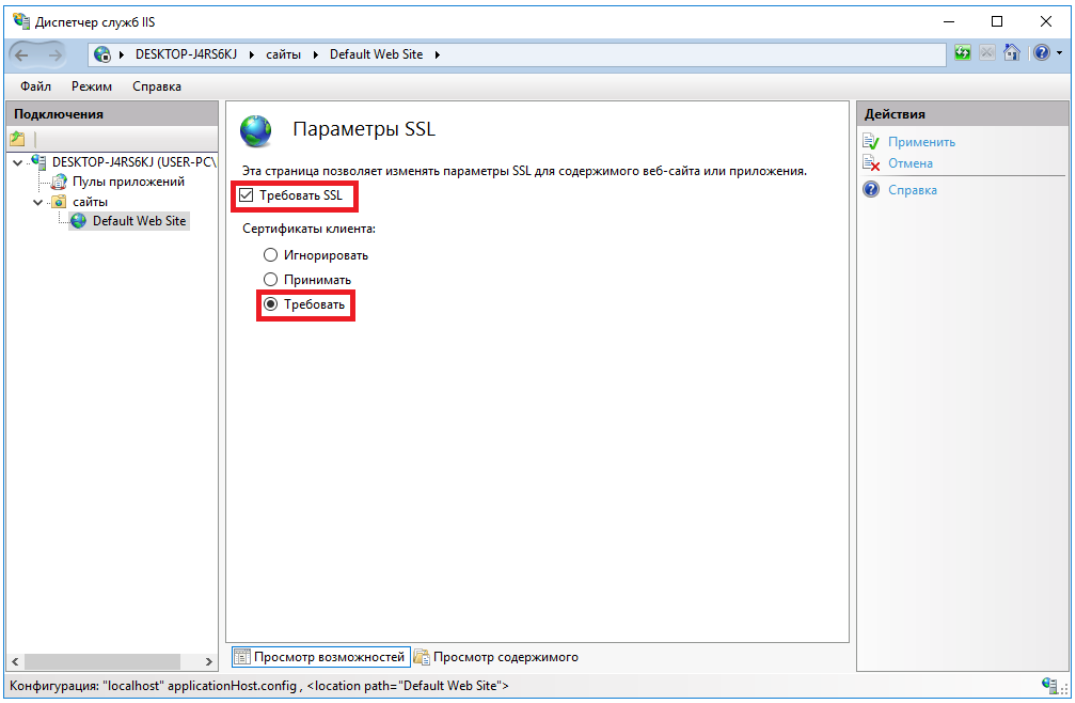


Рисунок 115. Параметры SSL для двусторонней аутентификации

4.5 Установка личного сертификата пользователя

Для успешной работы пользователя с сервером по протоколу TLS необходимо выполнить следующие действия:

1) Установить на компьютер пользователя КриптоПро CSP;

2) Выпустить личный сертификат пользователя, если он не был выпущен ранее и установить его в хранилище Личное текущего пользователя или на носитель другого типа, доступный для считывания на компьютере пользователя;

3) Выполнить проверку связи с сервером.

Используя установочный файл CSPSetup.exe установите КриптоПро CSP на компьютер пользователя (см. раздел Инсталляция СКЗИ КриптоПро CSP). Для решения текущей задачи достаточно принять при установке параметры, рекомендуемые по умолчанию.

Для выпуска и установки сертификата пользователя выполните действия, указанные в разд. 3, с учетом приведенных ниже рекомендаций.

Рекомендации по выпуску и установке сертификата пользователя:

- В поле **Имя** укажите имя пользователя.
- В поле **Тип сертификата** укажите «Сертификат проверки подлинности клиента».
- В секции **Параметры ключа** укажите «Использовать новый набор ключей» и выберите CSP.
- Если в дальнейшем предполагаются манипуляции с ключом сертификата, установите флаг «Пометить ключ как экспортируемый» и в дополнительных параметрах укажите понятное имя.
- Остальные параметры запроса оставьте по умолчанию.

Сертификат пользователя в составе контейнера закрытого ключа также может быть сохранен на различных типах носителей.

Для проверки правильности установки сертификата воспользуйтесь оснасткой для управления сертификатами КриптоПро. В меню Пуск выберите Все программы ⇒ КРИПТО-ПРО ⇒ Сертификаты. Сертификат пользователя должен находиться в хранилище Личное текущего пользователя (см. Рисунок 116).

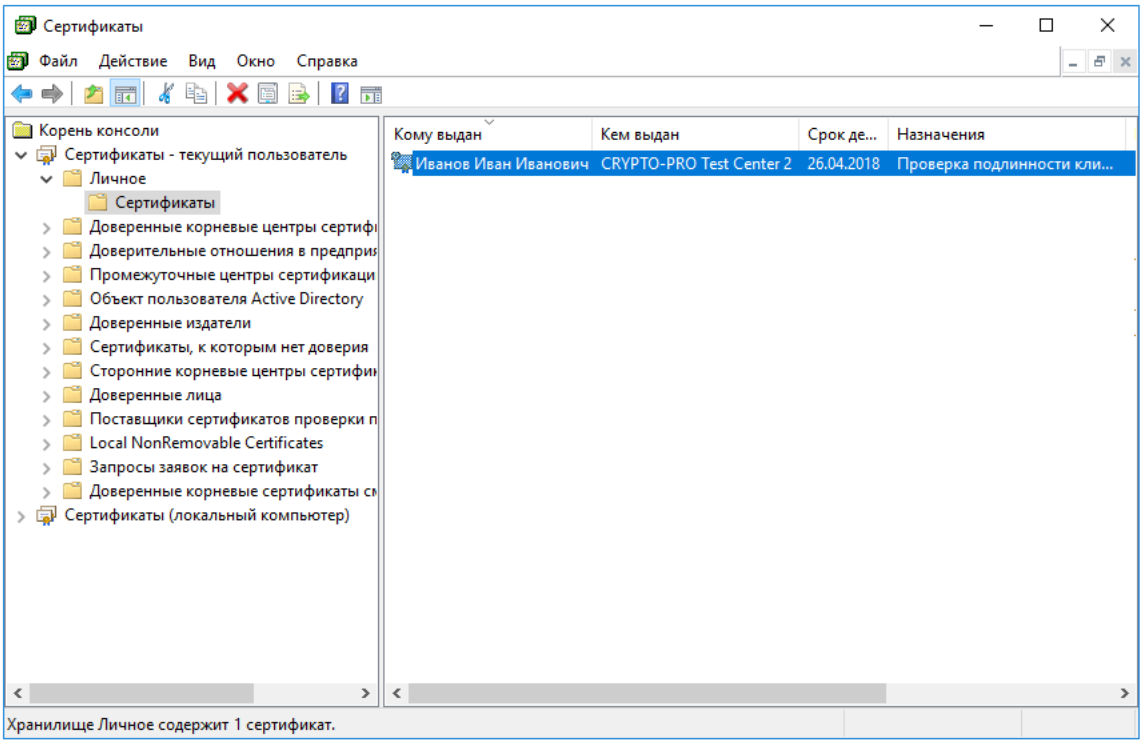


Рисунок 116. Проверка наличия сертификата пользователя в хранилище

4.6 Проверка двусторонней аутентификации клиент-сервер

Для проверки соединения с сервером по протоколу TLS нужно зайти через браузер на страницу сервера https://<domainname>/, где <domainname> — имя домена сервера.

Если настройка соединения выполнена правильно, то при переходе на страницу откроется диалог с выбором сертификата (см. Рисунок 117).

После выбора сертификата будет запрошен пароль к контейнеру сертификата пользователя. При вводе правильного пароля пользователю открывается доступ к сайту.

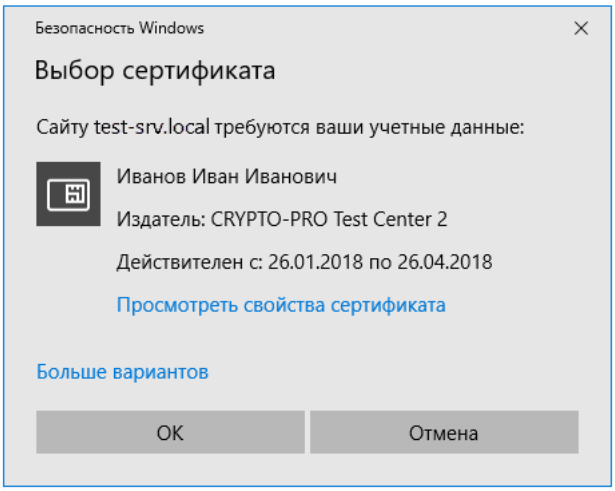


Рисунок 117. Выбор сертификата

Примечание. При получении сертификата пользователя необходимо убедиться в том, что поле «Улучшенный ключ» закладки Состав содержит значение «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)», а поле «Использование ключа» закладки Состав — значения «Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)». В случае отсутствия одного из этих значений в указанных полях двусторонняя аутентификация «клиент-сервер» может быть невозможна.

4.7 Настройка IIS на одновременное использование сертификатов ГОСТ и RSA

В случае, когда к одному веб-серверу необходимо настроить доступ по TLS со стороны клиентов, использующих различные браузеры, часть из которых имеет поддержку ГОСТ TLS, а часть — нет, можно настроить IIS на сервере на работу с двумя сертификатами сервера с различными криптоалгоритмами — ГОСТ и RSA. При этом на сервере будет использоваться один и тот же IP-адрес и порт для подключения клиентов.

Если сертификат сервера с алгоритмом RSA будет установлен с использованием одного из Microsoft RSA CSP , то следует использовать свойство shadow. Если же сертификат сервера с алгоритмом RSA планируется использовать с КриптоПро RSA CSP, то следует использовать свойство linked.

Отличие свойств shadow и linked заключается в том, что при shadow реализация TLS в варианте RSA выполняется с помощью Microsoft Schannel SSP, а для linked на стороне сервера всегда используется реализация TLS от КРИПТО-ПРО (и для ГОСТ, и для RSA).

4.7.1 Настройка и использование свойства shadow

1) Добавить на сервере необходимые сертификаты Центров Сертификации (ЦС), которые выдали сертификаты веб-сервера, в соответствующие хранилища локального компьютера — «Доверенные корневые ЦС» и «Промежуточные ЦС» (при наличии).

2) Установить сертификат сервера с алгоритмом ГОСТ в хранилище «Личные» локального компьютера с привязкой к ключу в контейнере с использованием криптопровайдера КриптоПро CSP: **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider** или **Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider**. **Примечание.** Не рекомендуется ставить пароль на этот контейнер, иначе придётся вводить его каждый раз после перезагрузки сервера в момент первого подключения клиента по TLS.

3) Установить сертификат RSA в хранилище «Личные» локального компьютера с привязкой к ключу в контейнере с использованием нужного криптопровайдера Microsoft CSP.

4) Отключить на сервере в панели управления КриптоПро CSP на вкладке **Настройки TLS** устаревшие cipher suite-ы в разделе Сервер (см. Рисунок 118).

Для применения изменений требуется перезагрузка сервера.

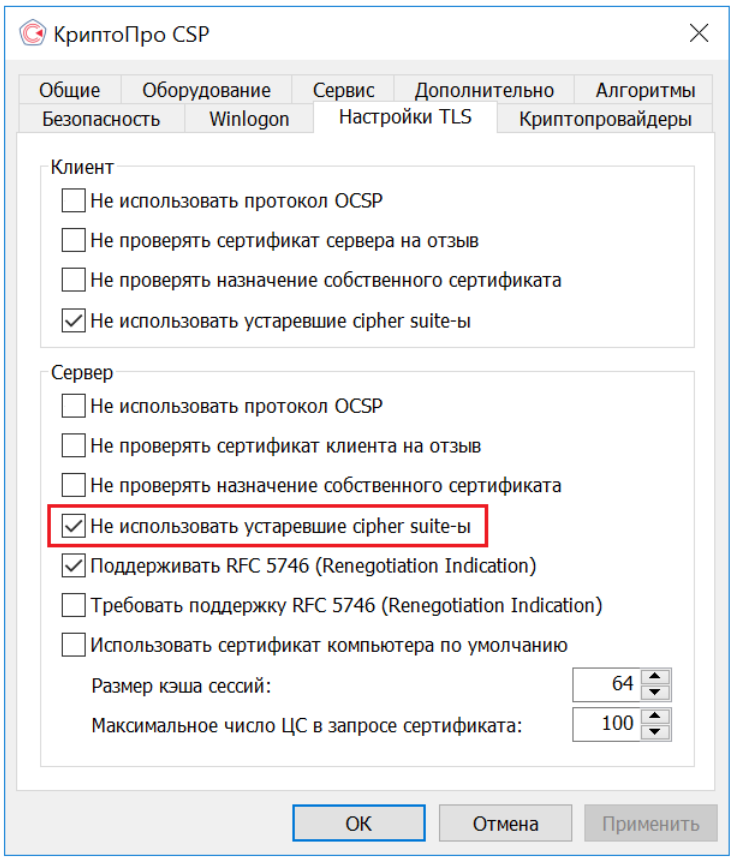


Рисунок 118. Отключение использования устаревших cipher suite на сервере

5) Запустить командную строку Windows (от имени администратора), перейти в папку установки КриптоПро CSP (по умолчанию `\Program Files\CryptoPro\CSP`) и выполнить команду:

```
csptest -property -machine -shadowthumbprint="отпечаток_сертификата_RSA"
-cert "отпечаток_сертификата_ГОСТ"
```

Примечание: При копировании отпечатков из окна просмотра свойств сертификата необходимо убедиться, что не скопированы непечатные символы в начале строки. Необходимо убрать пробелы внутри отпечатков (если есть), также пробелов не должно быть между названием опции `-shadowthumbprint` и ее значением (только знак =), например:

```
csptest -property -machine -shadowthumbprint=cdc6afd1eceae8cefd3689ebda4ad49e626ef776
-cert aae86068649073777590a604721382f2f2adc842
```

В опции `-cert` допустимо вместо отпечатка указать значение (или его часть) поля «Общее имя» («Common Name») сертификата сервера с алгоритмом ГОСТ. Если внутри значения есть пробелы, то значение нужно заключить в кавычки.

6) Сертификат веб-сервера с алгоритмом ГОСТ назначить в IIS в привязке на нужном веб-сайте.

Если этот сертификат веб-сервера с алгоритмом ГОСТ уже был ранее назначен в привязке на IIS, то после выполнения команды задания свойства *shadow* требуется повторно выбрать тот же сертификат ГОСТ в привязке на IIS.

После этого клиенты могут подключаться по ГОСТ TLS, если браузер его поддерживает. Если нет, то автоматически будет использоваться другой сертификат сервера, отпечаток которого был задан в свойстве *shadow*.

Чтобы проверить, установлено ли свойство *shadow* для сертификата ГОСТ в хранилище сертификатов «Личные» локального компьютера, можно использовать команду:

```
csptest -certprop -CERT "часть имени поля Common Name или отпечаток сертификата"
```

Например:

```
csptest -certprop -CERT aae86068649073777590a604721382f2f2adc842
```

Примечание: Написание названия опции большими буквами (-CERT) означает поиск в хранилище локального компьютера, а не текущего пользователя.

В выводе информации о сертификате будет указано:

```
Property # 65280 found->CP_CERT_SHADOW_CERT_PROP_ID id.
Thumbprint is: <значение_отпечатка_сертификата_RSA>
```

Клиенты должны доверять тем ЦС, которые выпустили соответствующие сертификаты сервера.

При использовании двустороннего TLS (когда браузер клиента предъявляет сертификат клиента) не все варианты сочетания криптоалгоритмов сертификатов сервера и клиента будут работать (см. таблицу совместимости браузеров табл. 1).

Таблица 1. Возможность подключения клиентов при использовании на сервере свойства *shadow*

	Internet Explorer 11	Chromium Gost 86.0.4240.198	Edge (chromium) 86.0.622.61	Chrome 86.0.4240.198
Односторонний tls	+	+	+	+
Двусторонний tls с сертификатом клиента ГОСТ	+	+	–	–
Двусторонний tls с сертификатом клиента на Microsoft RSA CSP	–	–	+	+
Двусторонний tls с сертификатом клиента на КриптоПро RSA CSP	Повторно спрашивает сертификат клиента и потом выдает ошибку	+	+	+

При необходимости очистить свойство *shadow* для ГОСТ сертификата сервера в хранилище «Личные» локального компьютера можно использовать команду без указания отпечатка сертификата RSA:

```
csptest -property  -machine -shadowthumbprint  -cert "отпечаток сертификата ГОСТ"
```

Если после этого будет нужно продолжать использовать тот же сертификат ГОСТ в IIS (уже без связки с сертификатом RSA), необходимо повторно выбрать тот же сертификат ГОСТ в привязке на IIS.

4.7.2 Настройка и использование свойства linked

1) Проверить, что установлен компонент поддержки RSA в КриптоПро CSP.

Откройте оснастку **Пуск** ⇒ **Панель управления** ⇒ **Программы** ⇒ **Программы и компоненты** ⇒ **Удаление или изменение программы**, щелкните правой кнопкой мыши на КриптоПро CSP и выберите действие Изменить. Компонент **Поддержка RSA/ECDSA криптопровайдеров** должен быть установлен (см. Рисунок 119).

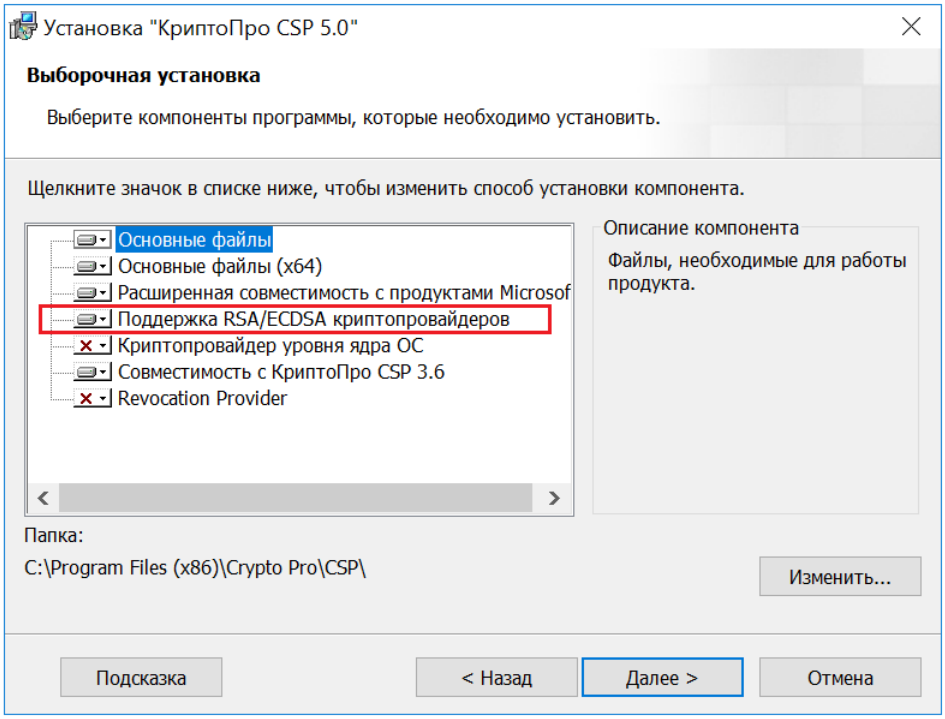


Рисунок 119. Установка компонента **Поддержка RSA/ECDSA криптопровайдеров**

2) Добавить на сервере необходимые сертификаты Центров Сертификации (ЦС), которые выдали сертификаты веб-сервера, в соответствующие хранилища локального компьютера — «Доверенные корневые ЦС» и «Промежуточные ЦС» (при наличии).

3) Установить сертификат сервера с алгоритмом ГОСТ в хранилище «Личные» локального компьютера с привязкой к ключу в контейнере с использованием криптопровайдера КриптоПро CSP: **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider** или **Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider**. **Примечание.** Не рекомендуется ставить пароль на этот контейнер, иначе придётся вводить его каждый раз после перезагрузки сервера в момент первого подключения клиента по TLS.

4) Установить сертификат RSA в хранилище «Личные» локального компьютера с привязкой к ключу в контейнере с использованием криптопровайдера КриптоПро RSA CSP: **Crypto-Pro Enhanced RSA and AES CSP**.

5) Отключить на сервере в панели управления КриптоПро CSP на вкладке **Настройки TLS** устаревшие cipher suite-ы в разделе Сервер (см. Рисунок 118).
Для применения изменений требуется перезагрузка сервера.

6) Запустить командную строку Windows (от имени администратора), перейти в папку установки КриптоПро CSP (по умолчанию `\Program Files\CryptoPro\CSP`) и выполнить команду:

```
csptest -property -machine -linkedthumbprint="отпечаток сертификата RSA"
-cert "отпечаток сертификата ГОСТ"
```

Примечание: При копировании отпечатков из окна просмотра свойств сертификата необходимо убедиться, что не скопированы непечатные символы в начале строки. Необходимо убрать пробелы внутри отпечатков (если есть), также пробелов не должно быть между названием опции `-linkedthumbprint` и ее значением (только знак =), например:

```
csptest -property -machine -linkedthumbprint=cdc6afd1eceae8cefd3689ebda4ad49e626ef776
-cert aae86068649073777590a604721382f2f2adc842
```

В опции `-cert` допустимо вместо отпечатка указать значение (или его часть) поля «Общее имя» («Common Name») сертификата сервера с алгоритмом ГОСТ. Если внутри значения есть пробелы, то значение нужно заключить в кавычки.

7) Сертификат веб-сервера с алгоритмом ГОСТ назначить в IIS в привязке на нужном веб-сайте.

Если этот сертификат веб-сервера с алгоритмом ГОСТ уже был ранее назначен в привязке на IIS, то после выполнения команды задания свойства *linked* требуется повторно выбрать тот же сертификат ГОСТ в привязке на IIS.

После этого клиенты могут подключаться по ГОСТ TLS, если браузер его поддерживает. Если нет, то автоматически будет использоваться другой сертификат сервера, отпечаток которого был задан в свойстве *linked*.

Чтобы проверить, установлено ли свойство *linked* для сертификата ГОСТ в хранилище сертификатов «Личные» локального компьютера, можно использовать команду:

```
csptest -certprop -CERT "часть имени поля Common Name или отпечаток сертификата"
```

Например:

```
csptest -certprop -CERT aae86068649073777590a604721382f2f2adc842
```

Примечание: Написание названия опции большими буквами (-CERT) означает поиск в хранилище локального компьютера, а не текущего пользователя.

В выводе информации о сертификате будет указано:

```
Property # 65281 found->CP_CERT_LINKED_CERT_PROP_ID id.
Thumbprint is: <значение отпечатка сертификата RSA>
```

Клиенты должны доверять тем ЦС, которые выпустили соответствующие сертификаты сервера.

При использовании двустороннего TLS (когда браузер клиента предъявляет сертификат клиента) не все варианты сочетания криптоалгоритмов сертификатов сервера и клиента будут работать (см. таблицу совместимости браузеров табл. 2).

Таблица 2. Возможность подключения клиентов при использовании на сервере свойства *linked*

	Internet Explorer 11	Chromium Gost 86.0.4240.198	Edge (chromium) 86.0.622.61	Chrome 86.0.4240.198
Односторонний tls	+	+	+	+
Двусторонний tls с сертификатом клиента ГОСТ	+	+	–	–
Двусторонний tls с сертификатом клиента на Microsoft RSA CSP	–	–	+	+
Двусторонний tls с сертификатом клиента на КриптоПро RSA CSP	Повторно спрашивает сертификат клиента и потом выдает ошибку	+	+	+

При необходимости очистить свойство *linked* для ГОСТ сертификата сервера в хранилище «Личные» локального компьютера можно использовать команду без указания отпечатка сертификата RSA:

```
csptest -property -machine -linkedthumbprint  -cert "отпечаток сертификата ГОСТ"
```

Если после этого будет нужно продолжать использовать тот же сертификат ГОСТ в IIS (уже без связки с сертификатом RSA), необходимо повторно выбрать тот же сертификат ГОСТ в привязке на IIS.

5 Описание использования, настроек и управления ключами в КриптоПро Winlogon

Для реализации первоначальной аутентификации пользователя протокола Kerberos V5 по сертификату и ключевому носителю, выпущенными в соответствии с алгоритмами ГОСТ Р 34.10-2001 или ГОСТ Р 34.10-2012 с использованием сертифицированного СКЗИ КриптоПро CSP, нужно выполнить следующие действия:

1) Установить и настроить контроллер домена на сервере (Active Directory Domain Services настраивается согласно стандартной документации Windows).

2) Установить СКЗИ КриптоПро CSP на сервер, на котором разворачивается контроллер домена, на сервер Центра сертификации (в случае, если служба ЦС располагается на отдельном сервере) и на компьютеры пользователей домена.

3) Установить и настроить службу сертификации Active Directory (ЦС).

4) Выпустить сертификат контроллера домена.

5) Выпустить сертификат Агента регистрации.

6) Выпустить смарт-карту пользователя домена.

Для работы КриптоПро Winlogon необходима специальная лицензия (для сервера и клиентского ПК). Эта лицензия может входить в лицензию КриптоПро CSP, или выдаваться отдельно. Ввести серийный номер лицензии можно с помощью утилиты Управление лицензиями КриптоПро PKI (подробнее см. разд. 2.3).

5.1 Установка и настройка службы сертификации Active Directory (Центр Сертификации)

Сертификаты контроллера домена и пользователей домена запрашиваются через оснастку **Сертификаты** на сервере, на котором настроен ЦС Предприятия (Enterprise CA) или через **веб-интерфейс Центра Сертификации** лицом, имеющим право выпуска сертификатов. Далее рассматривается вариант развертывания ЦС на сервере.

Перед установкой и настройкой ЦС Предприятия на сервере должен быть установлен КриптоПро CSP, также потребуются права группы Администраторы Предприятия (Enterprise Administrators).

Для установки ЦС Предприятия нужно добавить роль Центра сертификации. Для этого в диспетчере серверов нужно выбрать **Добавить роли и компоненты**. Запустится Мастер добавления ролей и компонентов. На шаге выбора роли сервера необходимо установите флаг **Службы сертификатов Active Directory** (см. Рисунок 120) и нажмите кнопку **Далее**.

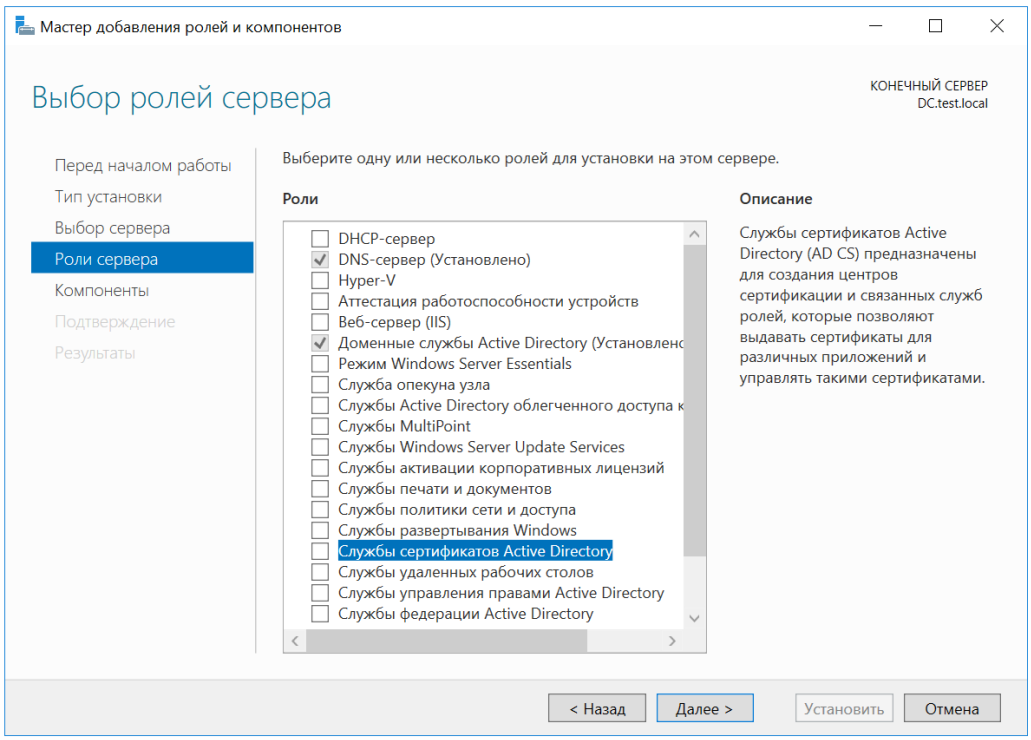


Рисунок 120. Добавление роли ЦС

При этом мастером предлагается добавить компоненты, необходимые для службы сертификатов Active Directory (см. Рисунок 121). Для установки компонентов по умолчанию нажмите кнопку **Добавить компоненты**.

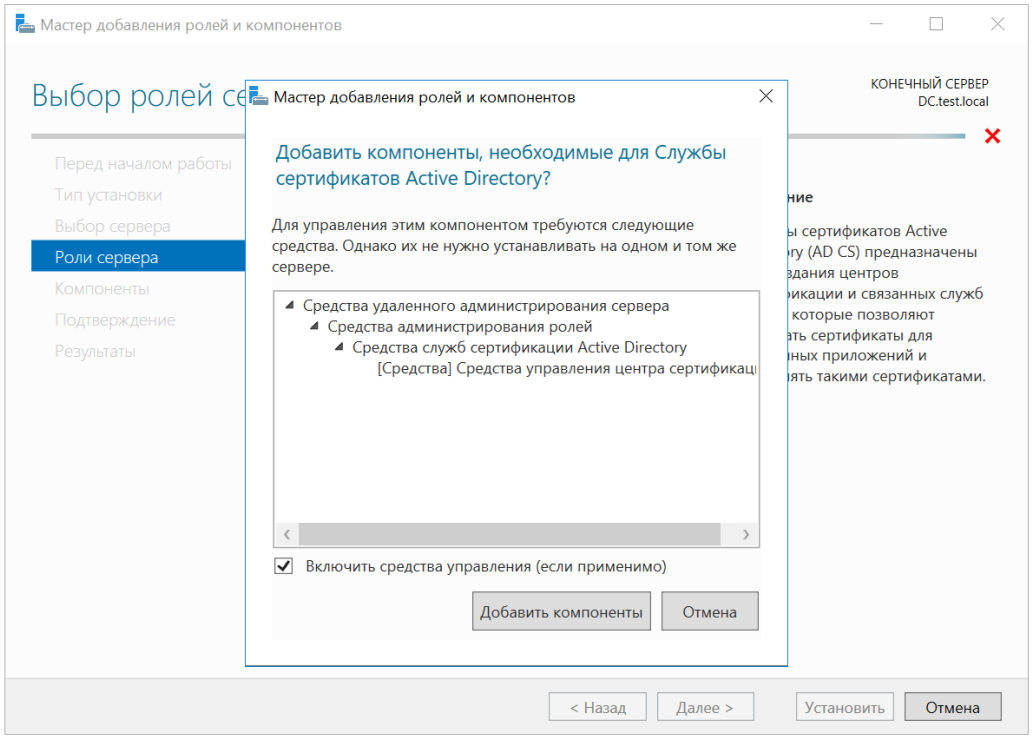


Рисунок 121. Добавление компонентов для роли ЦС

На следующем шаге выберите для установки службу ролей **Центр сертификации** и нажмите кнопку **Далее** (см. Рисунок 122).

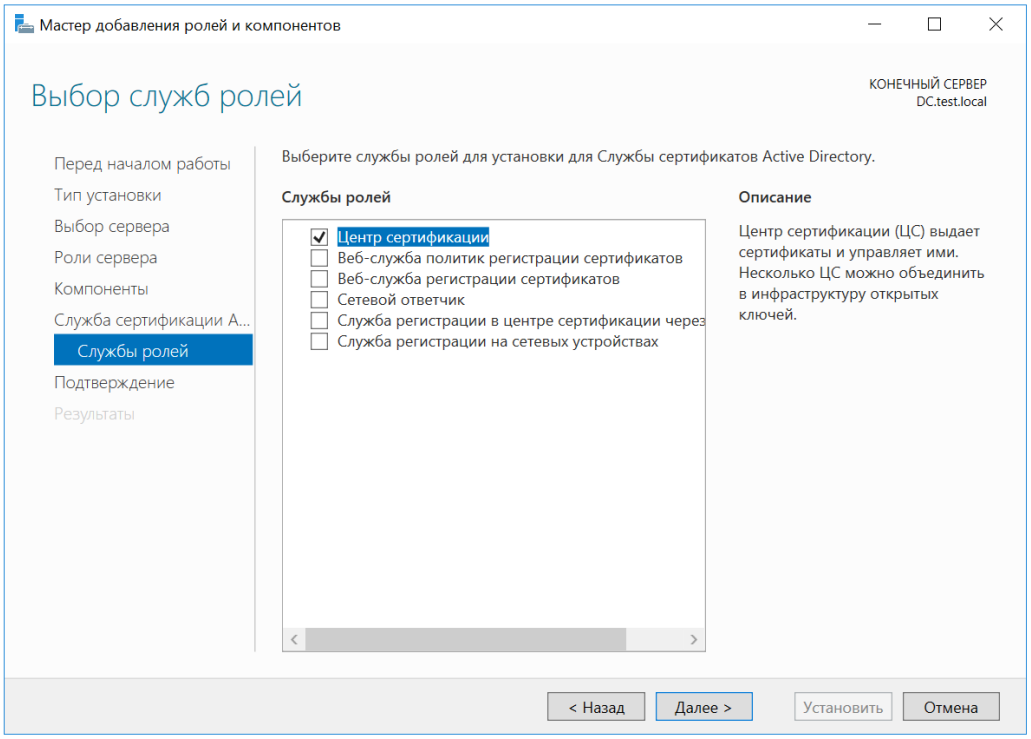


Рисунок 122. Добавление компонентов для роли ЦС

В окне «Подтверждение установки компонентов» после просмотра выбранных для установки компонентов нажмите кнопку **Установить** (см. Рисунок 123).

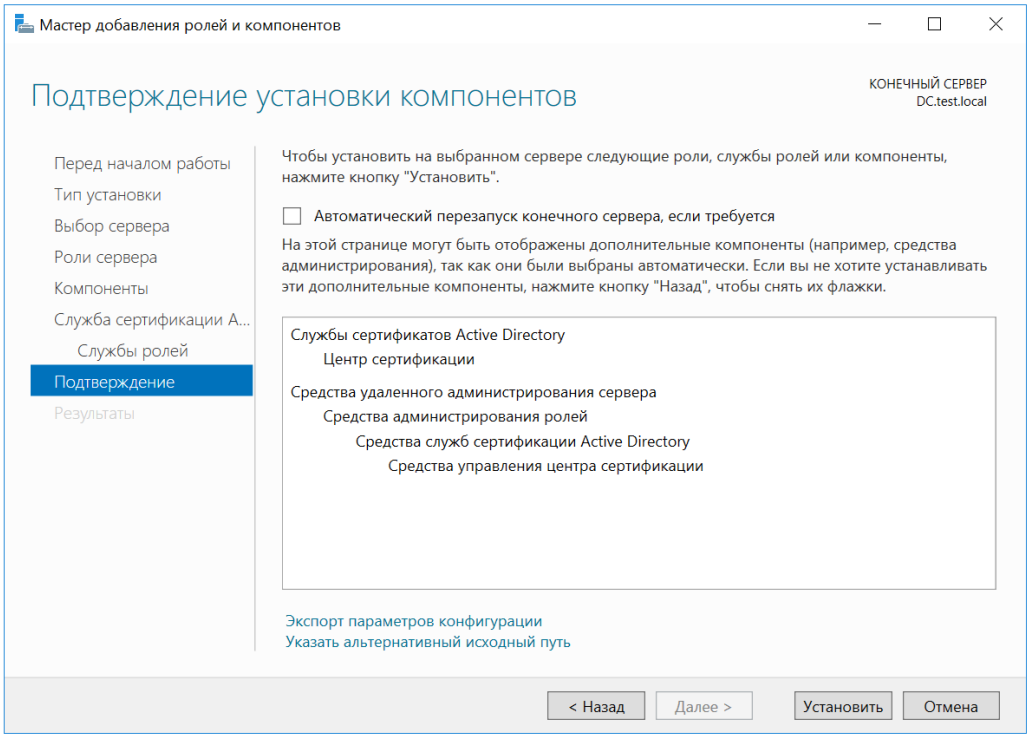


Рисунок 123. Подтверждение установки компонентов роли ЦС

По окончании установки компонентов, требующихся для роли Центра сертификации, необходимо настроить службы сертификатов. Для этого в окне «Ход установки» нажмите кнопку **Настроить службы сертификатов Active**

Directory на конечном сервере (см. Рисунок 124).

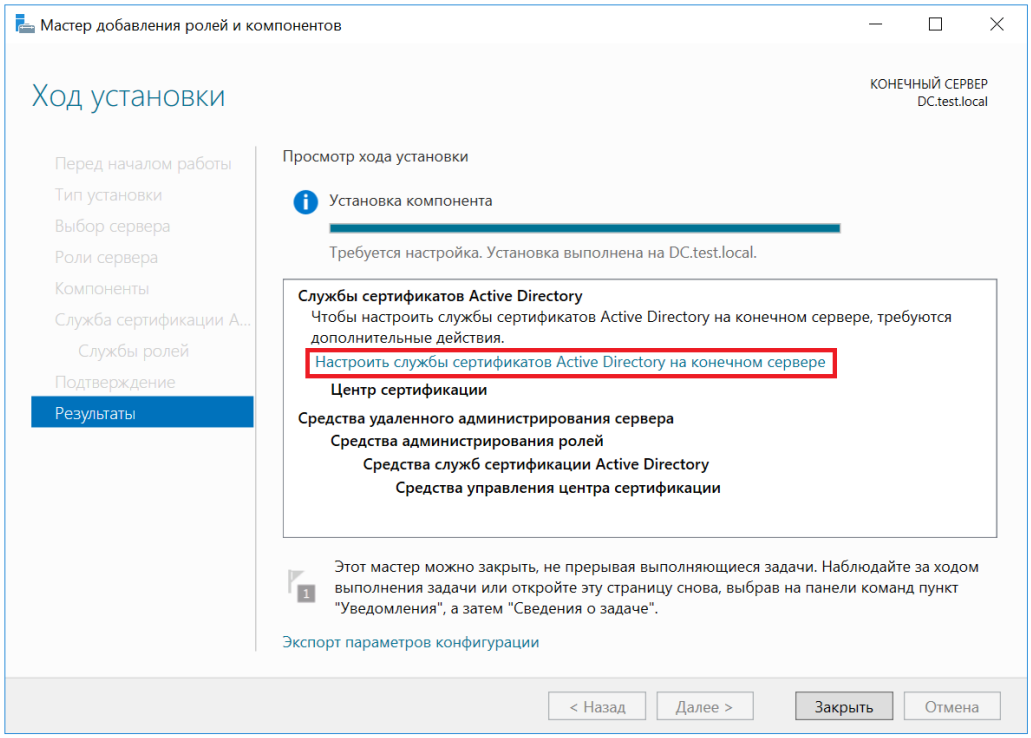


Рисунок 124. Настройка службы сертификатов AD на конечном сервере

Откроется Мастер конфигурации службы сертификатов Active Directory. Укажите учетные данные для настройки и нажмите кнопку **Далее** (см. Рисунок 125).

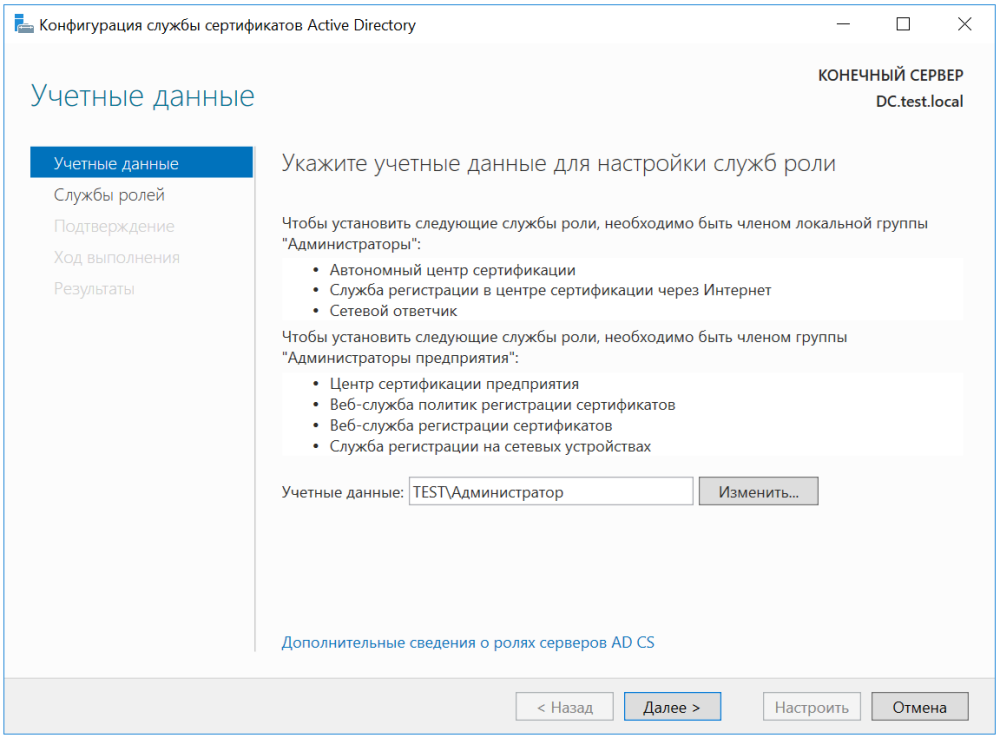


Рисунок 125. Учетные данные службы сертификатов AD

В окне «Службы ролей» установите флаг **Центр сертификации** и нажмите кнопку **Далее** (см. Рисунок 126).

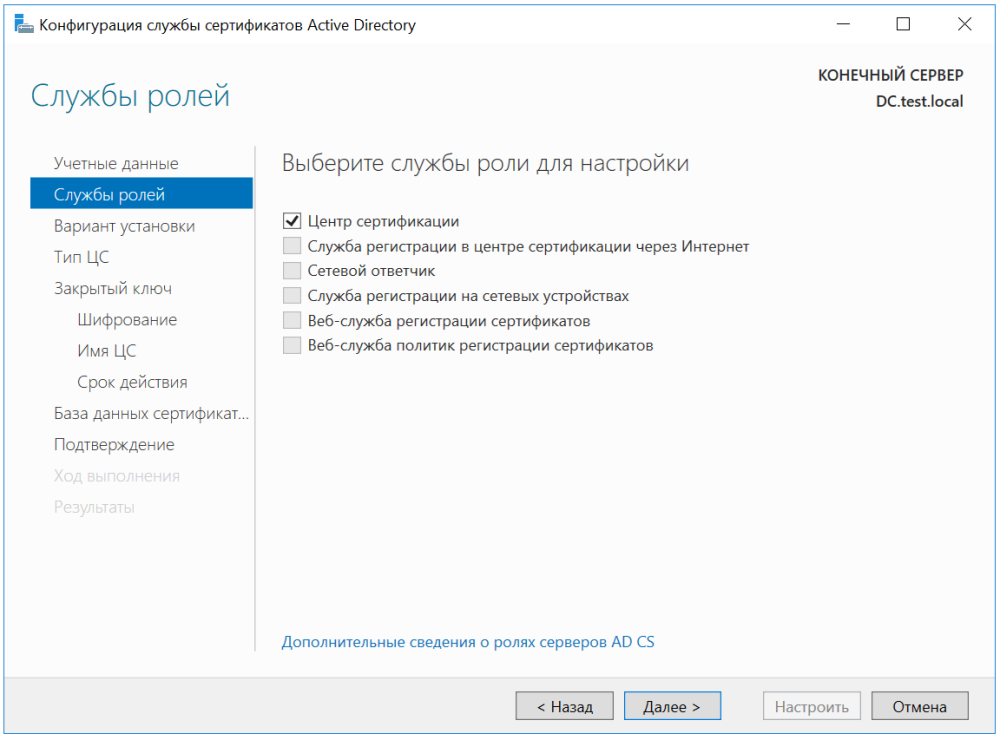


Рисунок 126. Выбор службы роли для настройки ЦС

В окне «Вариант установки» выберите подходящий вариант установки ЦС и нажмите кнопку **Далее** (см. Рисунок 127).

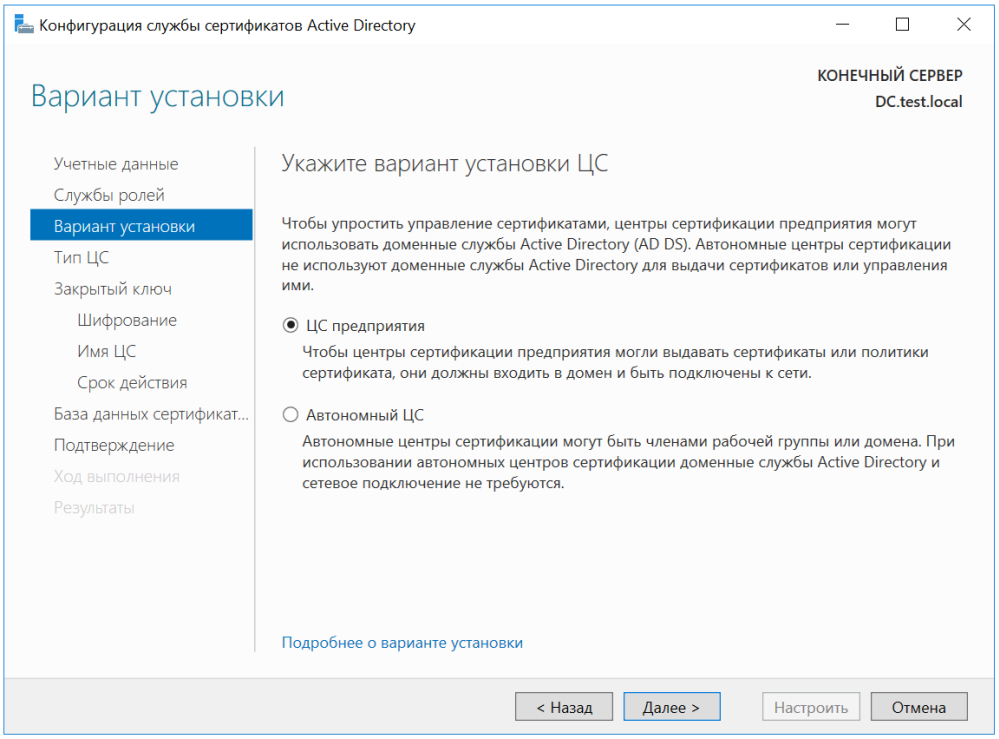


Рисунок 127. Выбор варианта установки ЦС

В окне «Тип ЦС» укажите тип ЦС и нажмите кнопку **Далее** (см. Рисунок 128).

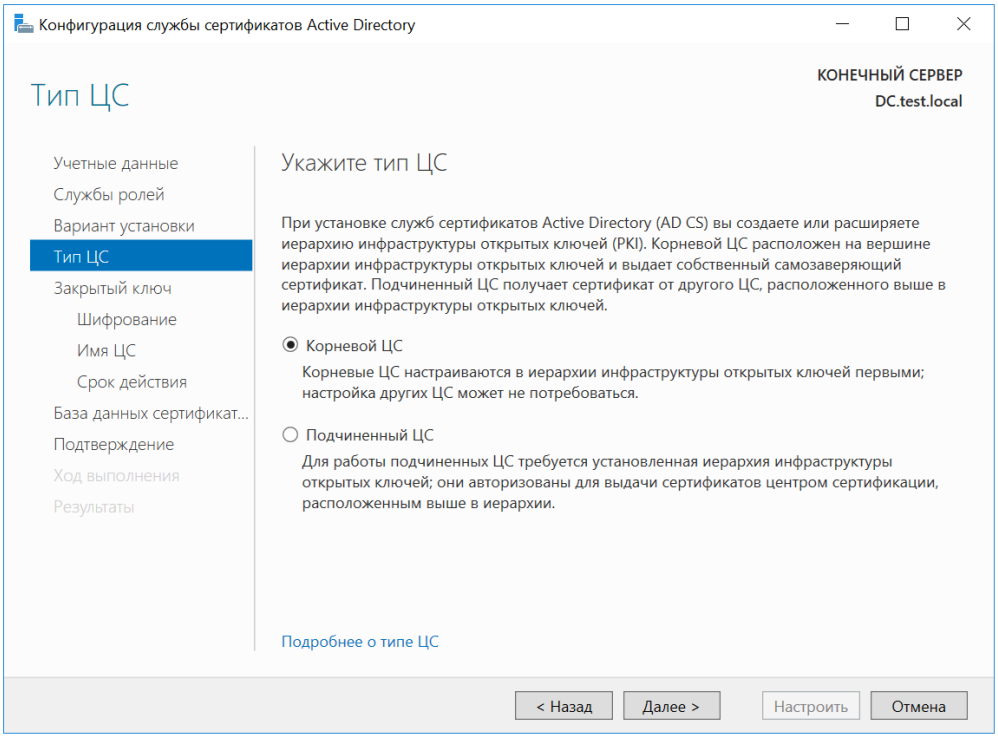


Рисунок 128. Выбор типа ЦС

В окне «Закрытый ключ» выберите опцию **Создать закрытый ключ** и нажмите кнопку **Далее** (см. Рисунок 129).

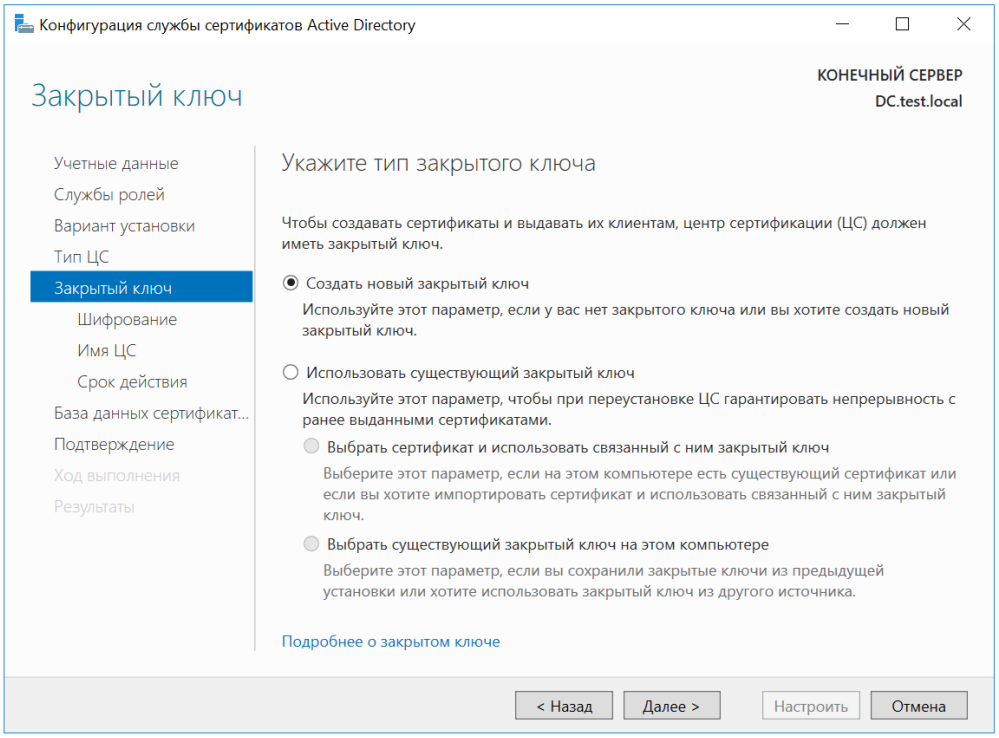


Рисунок 129. Выбор типа закрытого ключа для ЦС

В окне «Шифрование для ЦС» выберите из списка поставщика служб шифрования и установите флаг **Разрешить**

взаимодействие с администратором, если ЦС обращается к закрытому ключу. Нажмите кнопку **Далее** (см. Рисунок 130).

Примечание. В некоторых версиях Windows Server данный флаг называется **Разрешить CSP доступ к рабочему столу**. Если это свойство отключено, системные службы не смогут взаимодействовать с рабочим столом пользователя, который вошел в систему.

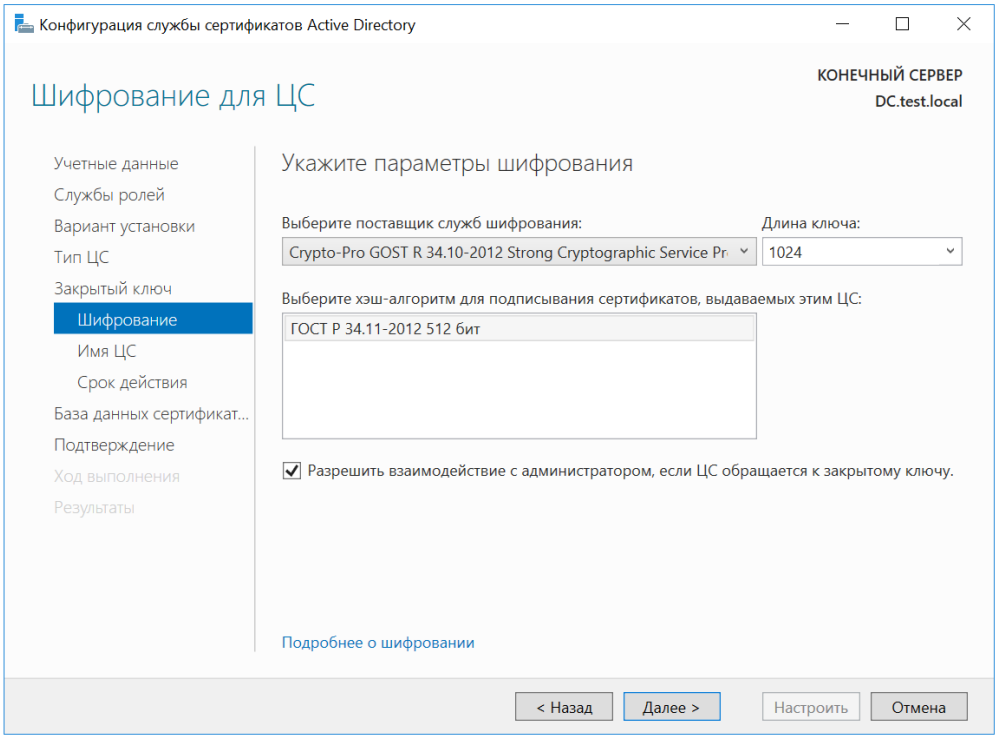


Рисунок 130. Выбор параметров шифрования для ЦС

В окне «Имя ЦС» укажите общее имя для ЦС и нажмите кнопку **Далее** (см. Рисунок 131).

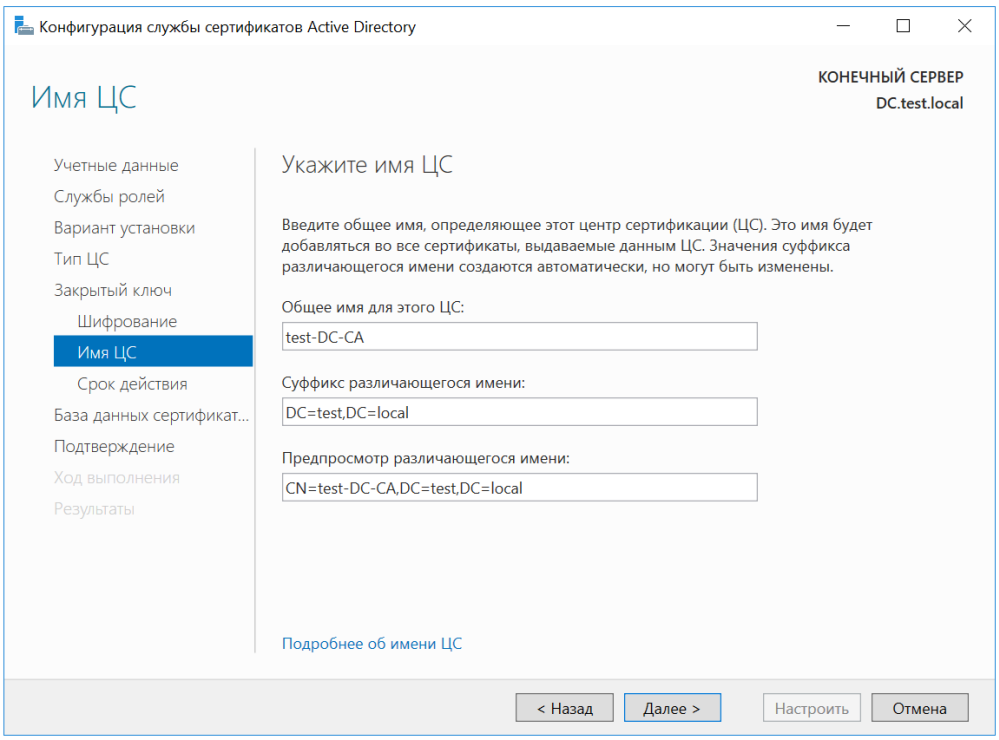


Рисунок 131. Ввод общего имени ЦС

На следующем шаге укажите срок действия ключа и расположение базы данных сертификатов.

Все указанные параметры ещё раз выводятся в окне «Подтверждение». Нажмите кнопку **Настроить** для того, чтобы сконфигурировать службы в соответствии с заданными параметрами (см. Рисунок 132).

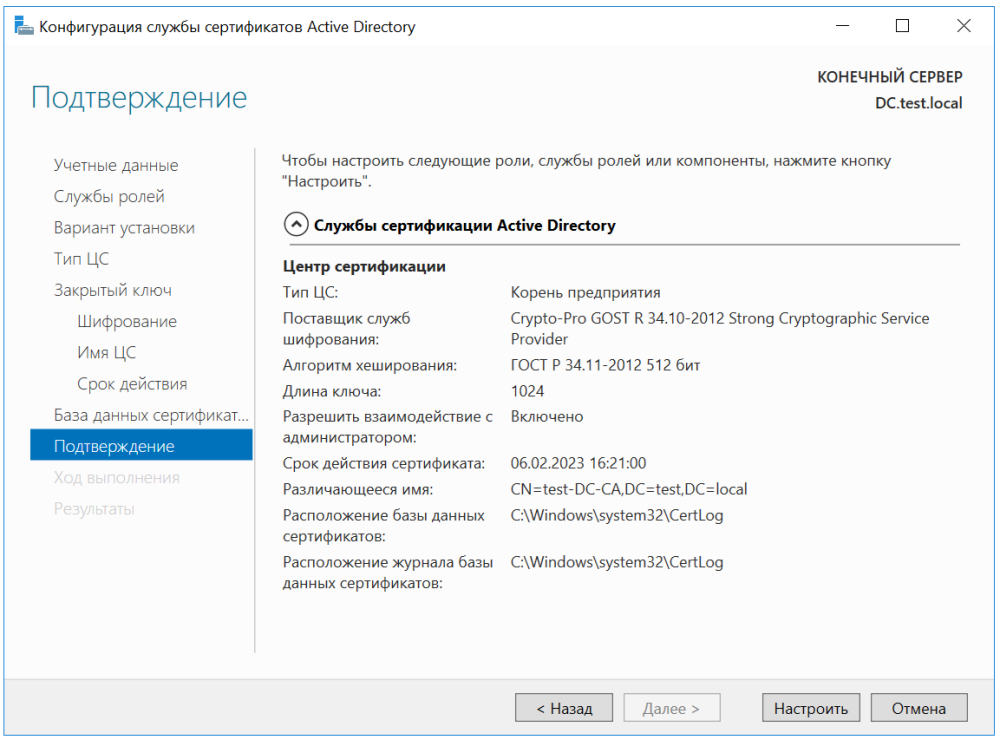


Рисунок 132. Подтверждение параметров ЦС

В процессе создания закрытого ключа для ЦС выводится окно Биологического ДСЧ (см. Рисунок 133) и криптопровайдер запрашивает пароль на создаваемый контейнер (пароль в данном случае указывать не нужно).

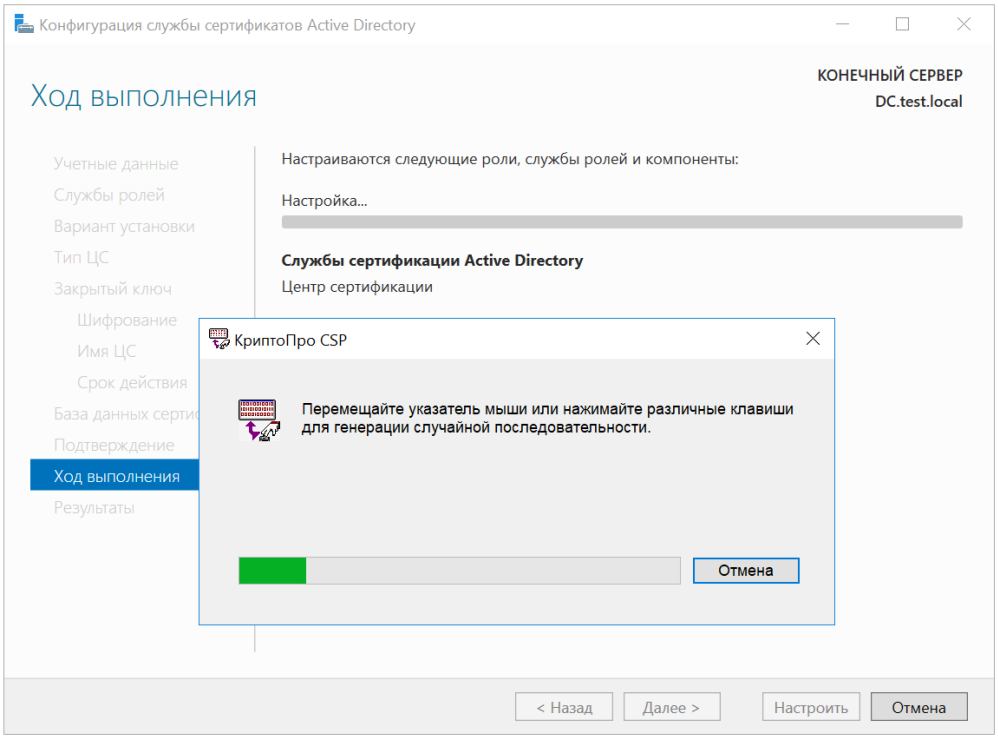


Рисунок 133. Выполнение конфигурирования ЦС

После выполнения данной задачи корневой сертификат ЦС можно увидеть в хранилище **Доверенные корневые центры сертификации** Локального компьютера через оснастку **Сертификаты** (см. Рисунок 134).

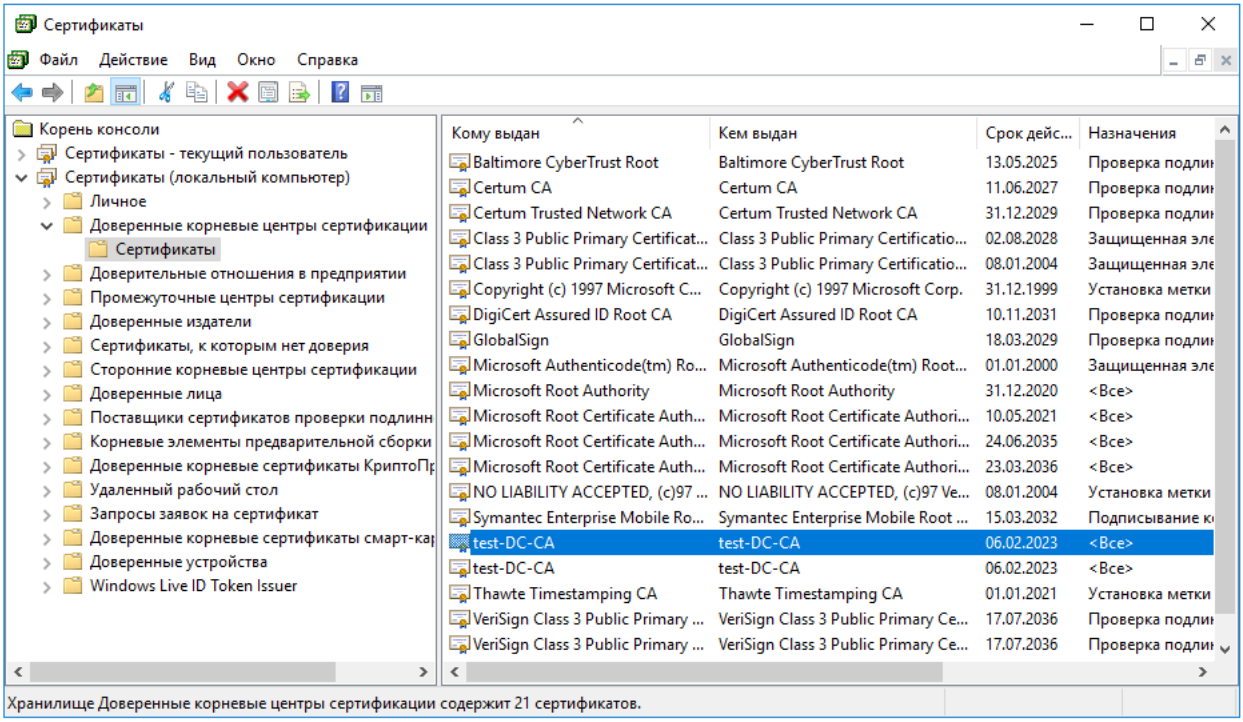


Рисунок 134. Корневой сертификат ЦС

Примечание. Если изменения не вступили в силу, для обновления групповой политики в командной строке выполните `gpupdate/force`.

5.2 Добавление шаблонов сертификатов на сервере

Для того, чтобы контроллер домена поддерживал Winlogon, необходимо выпустить сертификат для контроллера домена. Чтобы пользователь с ролью Агента регистрации мог производить выпуск сертификатов для других пользователей, необходимо выпустить сертификаты Агента регистрации и Входа по смарт-карте.

Шаблоны для вышеуказанных сертификатов по умолчанию могут быть отключены, поэтому нужно проверить их наличие в списке шаблонов сертификатов и включить недостающие. Для этого на сервере, на котором установлена служба ЦС, откройте оснастку Центра сертификации (**Пуск** ⇒ **Панель управления** ⇒ **Администрирование** ⇒ **Центр Сертификации**). В список шаблонов сертификатов необходимо включить шаблоны:

- Контроллер домена;
- Агент регистрации;
- Вход со смарт-картой.

Для этого выберите **Шаблоны сертификатов**, затем из контекстного меню **Создать** ⇒ **Выдаваемый шаблон сертификата** (см. Рисунок 135).

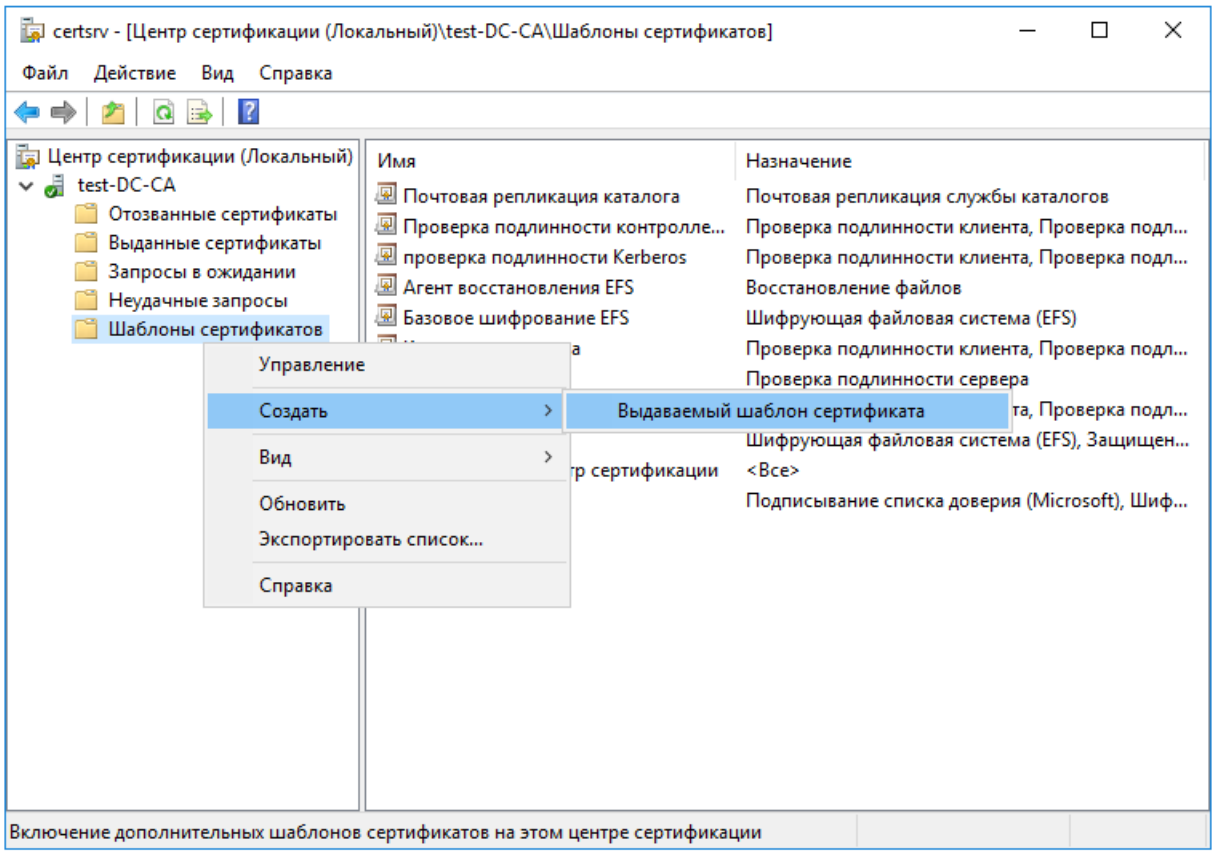


Рисунок 135. Добавление шаблонов сертификатов

В окне включения шаблонов сертификатов выделите необходимые шаблоны (возможен множественный выбор при удержании клавиши Ctrl) и нажмите кнопку **OK** (см. Рисунок 136).

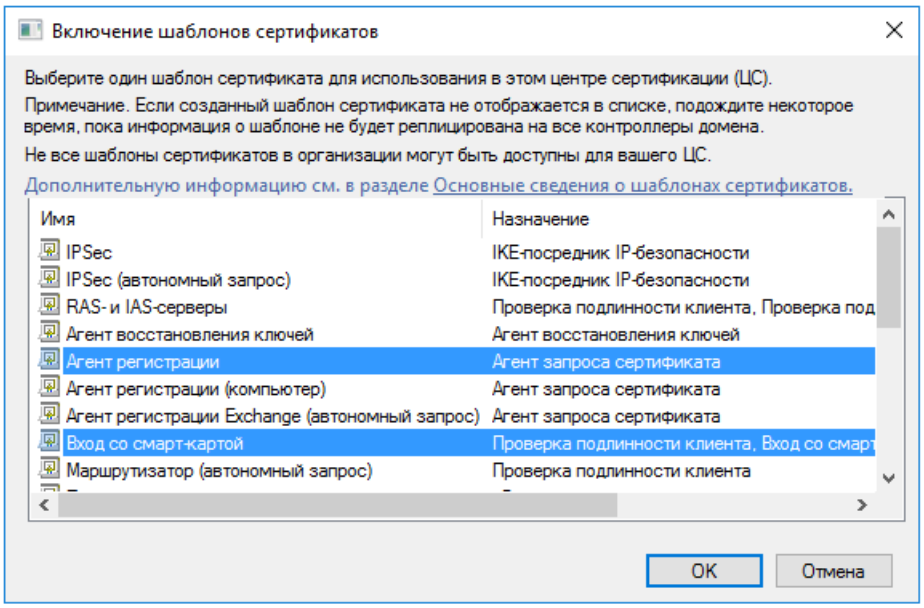


Рисунок 136. Включение шаблонов сертификатов

Далее администратору домена необходимо обновить шаблоны через Панель управления СКЗИ КриптоПро CSP. Для этого на вкладке **Winlogon** нужно нажать кнопку **Шаблоны** (см. Рисунок 137).

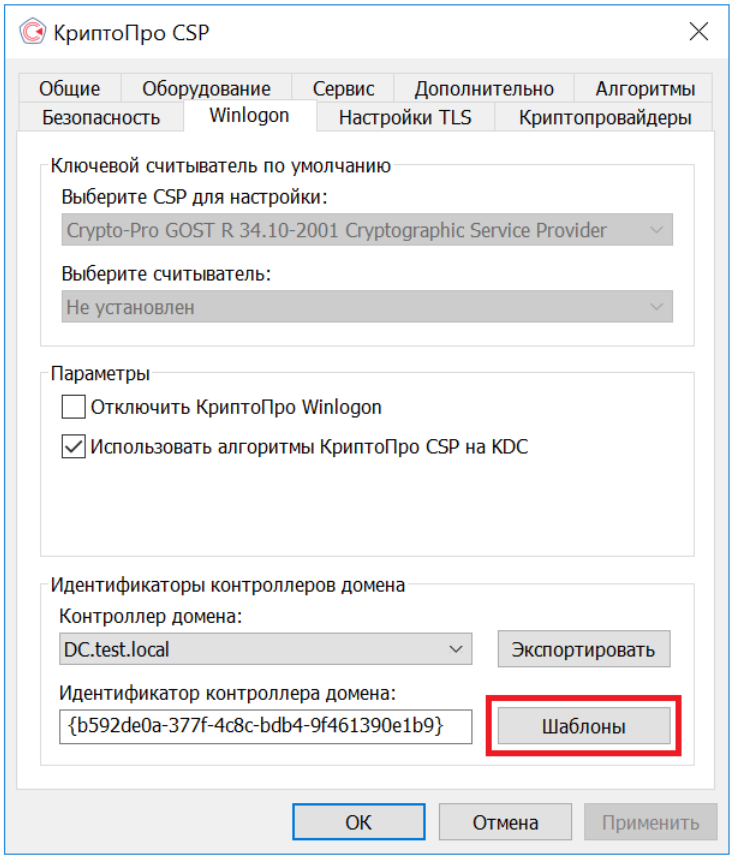


Рисунок 137. Обновление шаблонов в панели управления

После выполнения этого действия появится сообщение о том, что все шаблоны успешно обновлены, можно будет приступать к созданию заявок на сертификаты.

Если редактируются или добавляются новые шаблоны для контроллера домена и агента регистрации, данное действие нужно производить в обязательном порядке.

5.2.1 Настройка шаблонов сертификатов

Для того, чтобы сертификаты можно было использовать в Winlogon, нужно, чтобы они удовлетворяли определённым требованиям к сертификатам Контроллера домена, Агента регистрации, Входа по смарт-карте. Подробнее данные требования описаны в документации Microsoft.

Если существующий шаблон не удовлетворяет требованию к составу сертификата, необходимо его изменить. Для этого нужно создать копию шаблона, отредактировать её и включить в список шаблонов ЦС.

Откройте оснастку Центра сертификации (**Пуск** ⇒ **Панель управления** ⇒ **Администрирование** ⇒ **Центр сертификации**). В оснастке выберите свой ЦС, откройте **Шаблоны сертификатов**. В контекстном меню нажмите **Управление** (см. Рисунок 138).

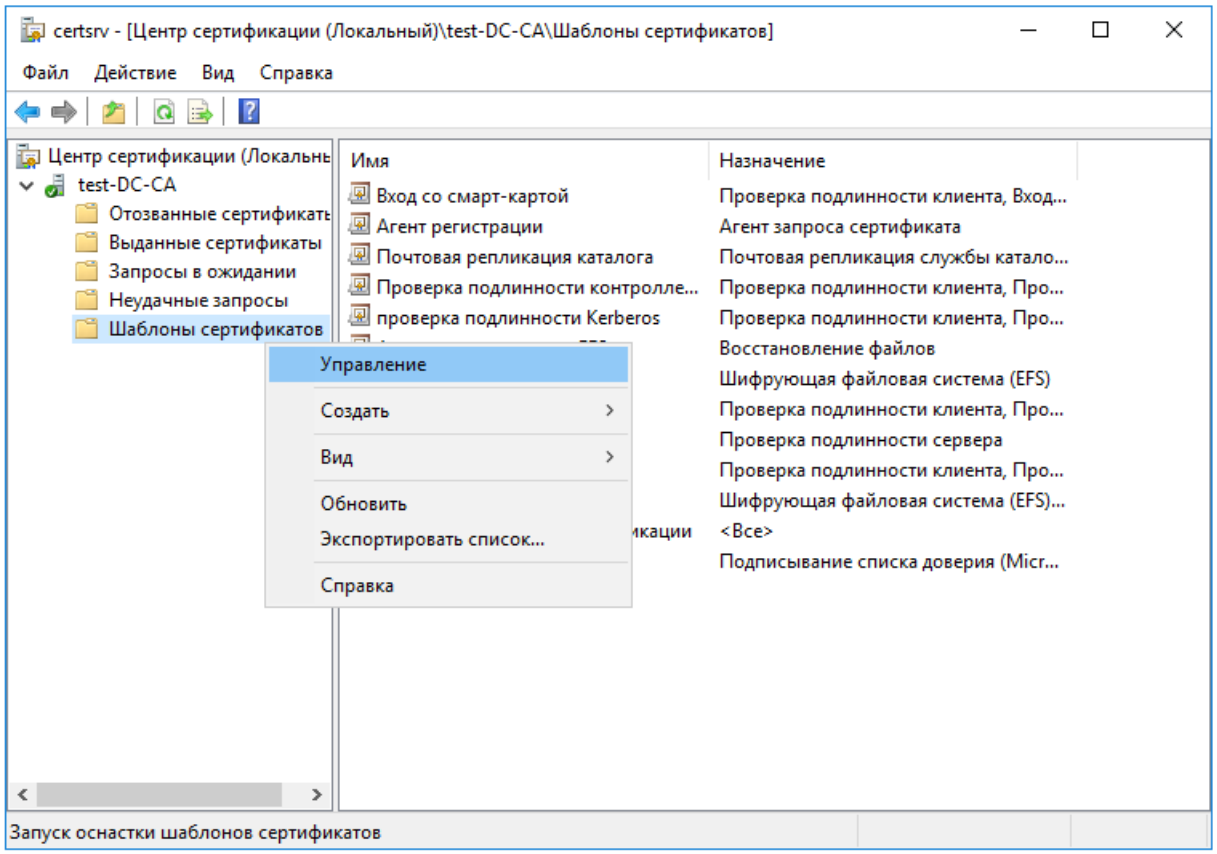


Рисунок 138. Управление шаблонами сертификатов

Запустится оснастка шаблонов сертификатов. Выберите редактируемый шаблон и нажмите в контекстном меню кнопку **Скопировать шаблон** (см. Рисунок 139).

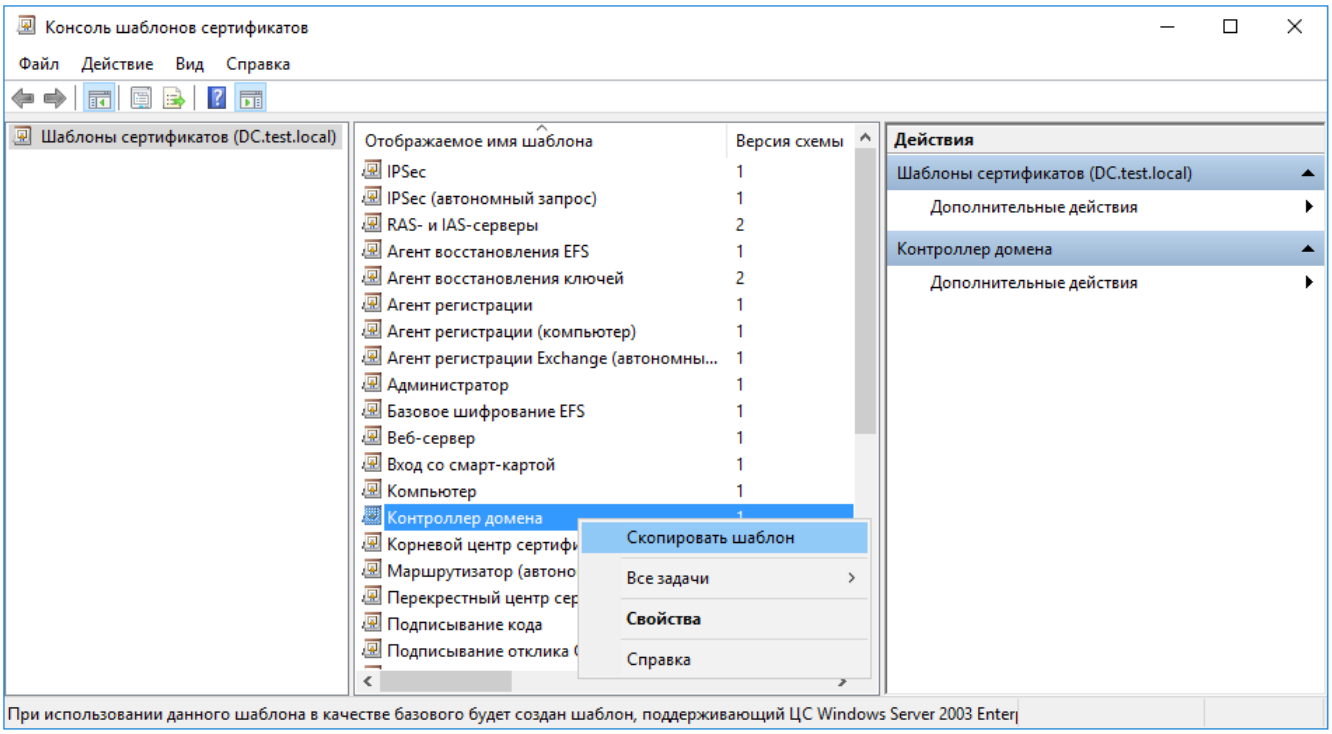


Рисунок 139. Консоль шаблонов сертификатов

Откроется форма, в которой можно изменить свойства шаблонов так, чтобы они соответствовали требованиям, описанным в разд. 5.3.1, разд. 5.5.1 (см. Рисунок 140).

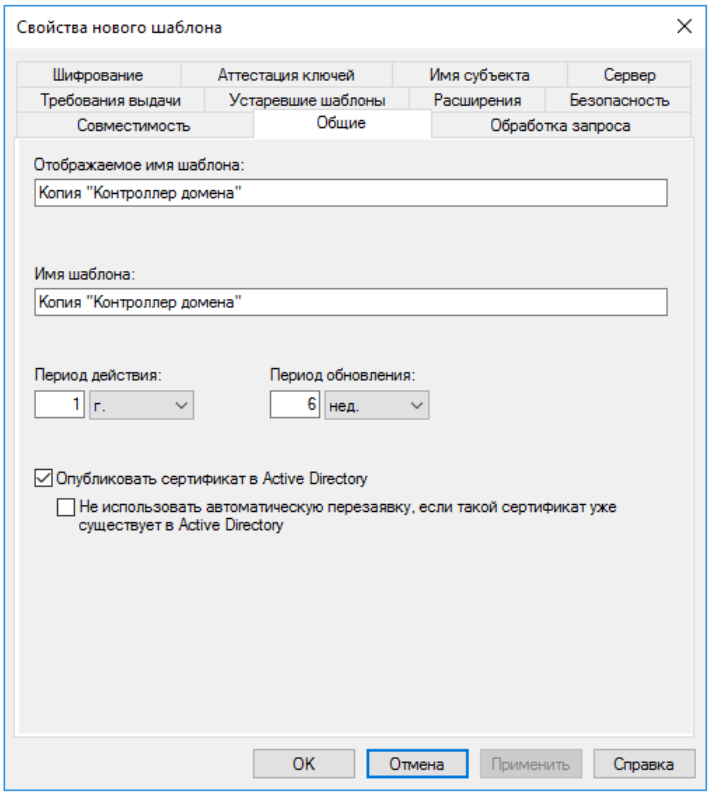


Рисунок 140. Свойства нового шаблона

После сохранения нового шаблона нужно добавить его через список шаблонов способом, описанным в разд. 5.2.

5.3 Выпуск сертификата контроллера домена

Выпуск сертификата контроллера домена должен производиться на сервере, на котором развёрнуты службы AD, пользователем с правами администратора домена. Для этого через меню Пуск откройте оснастку **Сертификаты**, затем в хранилище Личное Локального компьютера выполните **Все задачи** ⇒ **Запросить новый сертификат** (см. Рисунок 141).

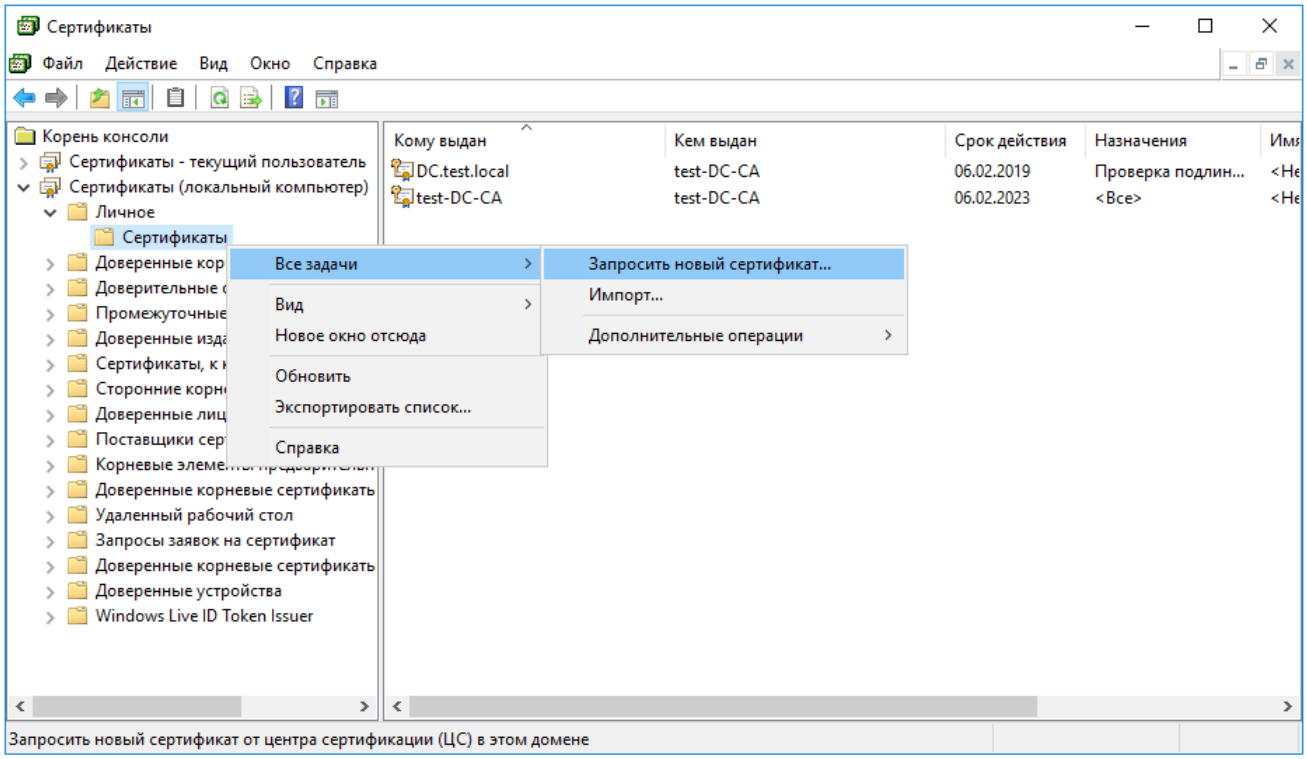


Рисунок 141. Запрос сертификата контроллера домена

Откроется Мастер регистрации сертификатов. Нажмите кнопку **Далее** (см. Рисунок 142).

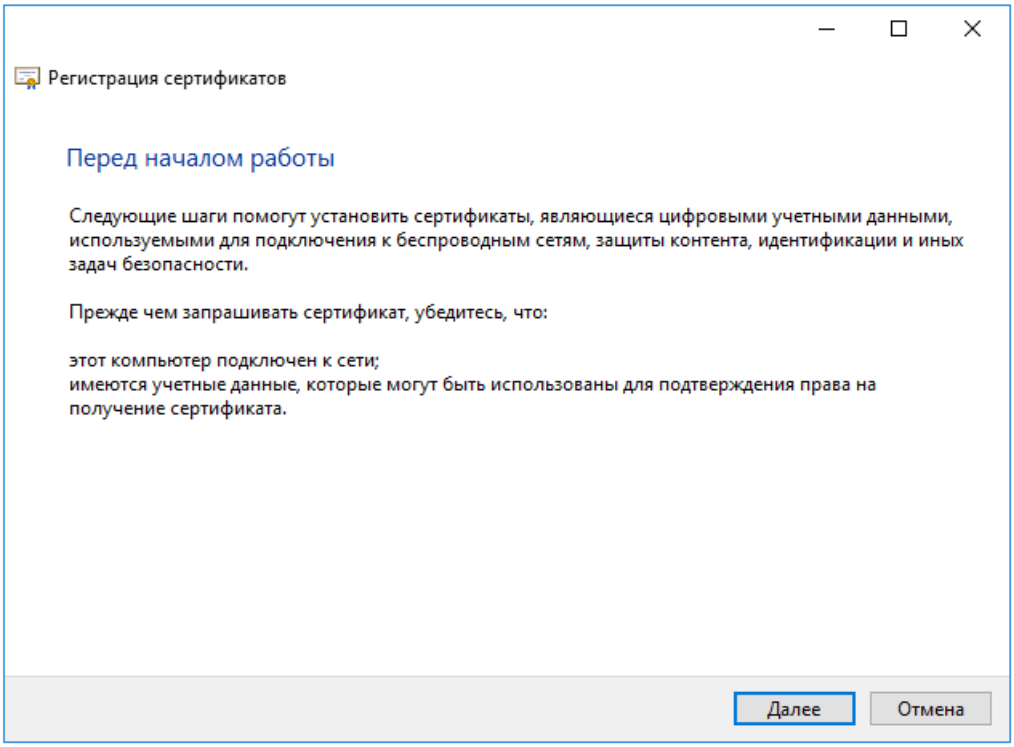


Рисунок 142. Мастер регистрации сертификатов

В окне «Выбор политики регистрации сертификатов» оставьте параметры по умолчанию и перейдите к следующему шагу, нажав кнопку **Далее** (см. Рисунок 143).

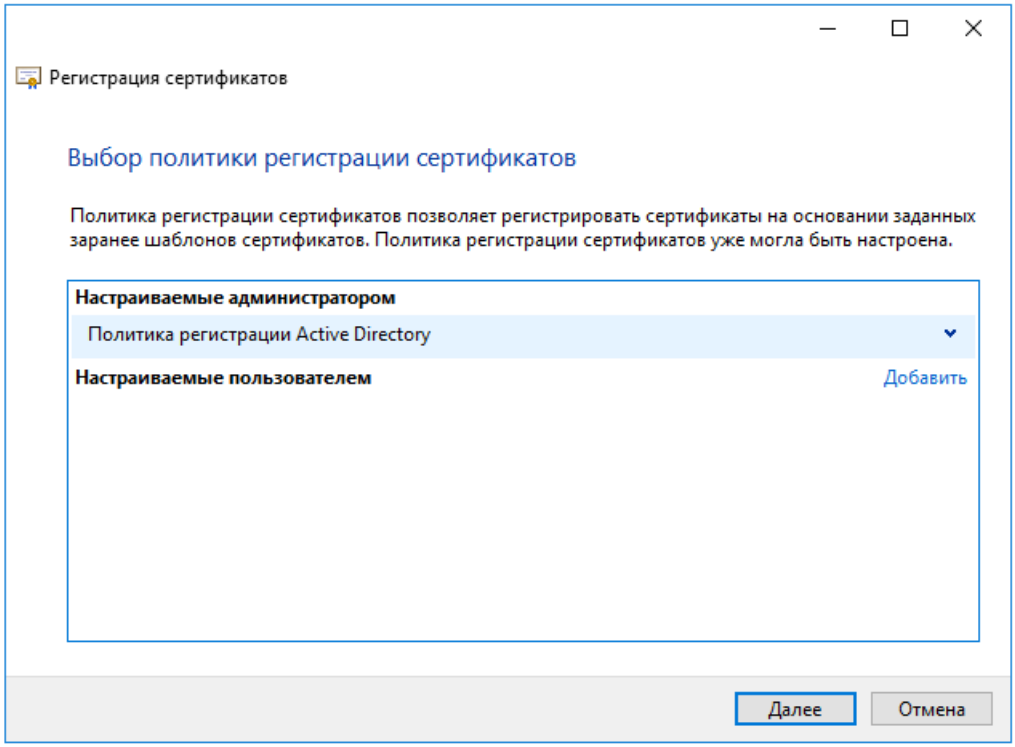


Рисунок 143. Выбор политики регистрации сертификатов

В окне «Запрос сертификатов» из списка типов сертификатов выберите Контроллер домена (см. Рисунок 144).

Проверьте правильность заполненных данных и при необходимости выберите поставщика службы шифрования в **Свойствах** на вкладке **Закрытый ключ** (см. Рисунок 145). Для выпуска сертификата на контроллер домена нажмите кнопку **Заявка**.

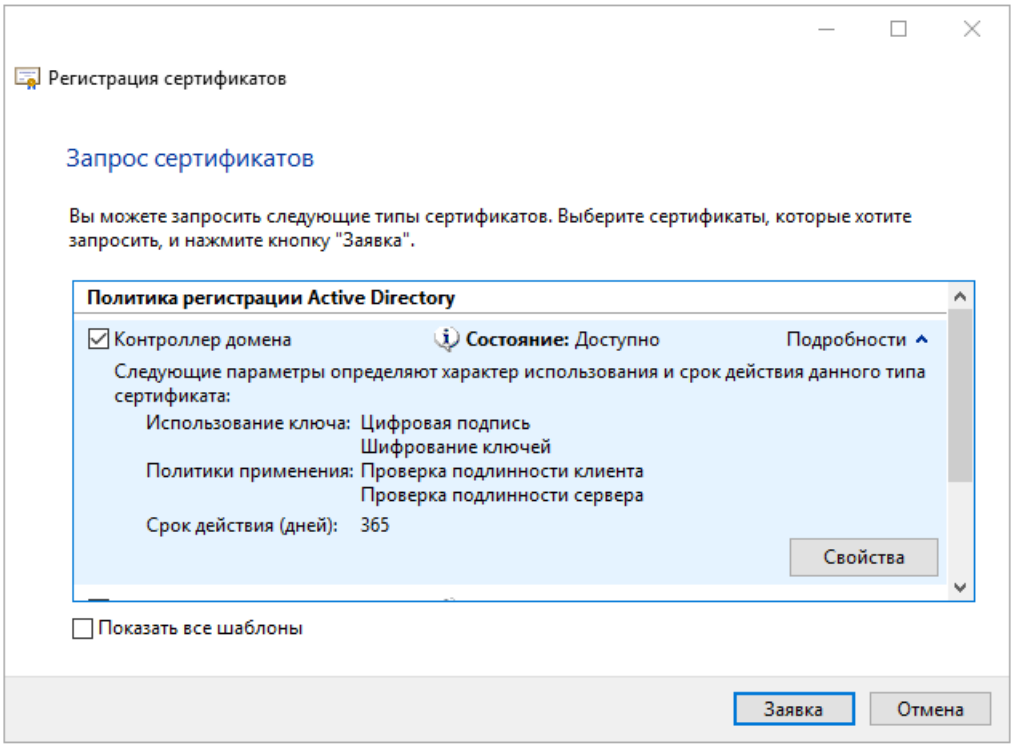


Рисунок 144. Запрос сертификата контроллера домена

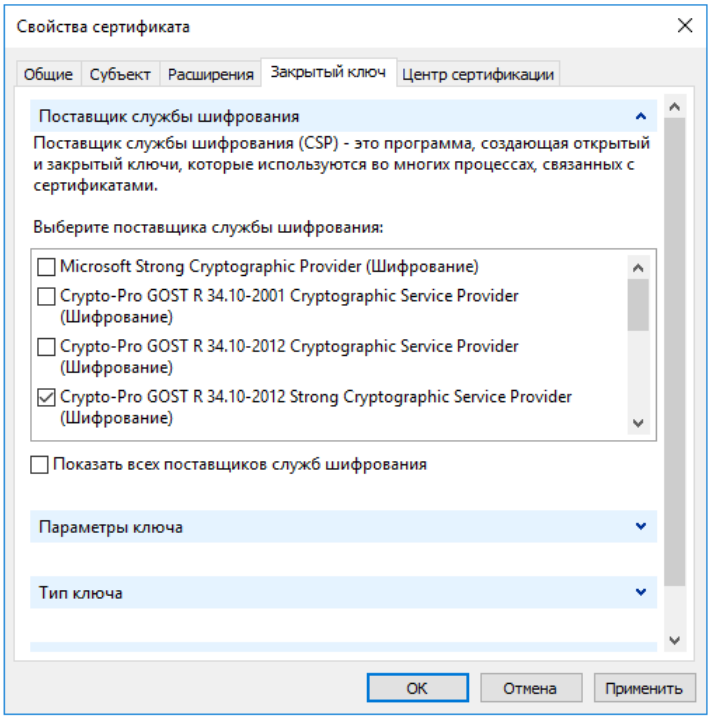


Рисунок 145. Выбор поставщика службы шифрования

При выпуске сертификата предлагается установить новый пароль на контейнер. В процессе создания закрытого

ключа для контроллера домена выводится окно Биологического ДСЧ и криптопровайдер запрашивает пароль на создаваемый контейнер (пароль в данном случае указывать не нужно). После завершения работы Биологического ДСЧ откроется окно, информирующее об успешной установке сертификата (см. Рисунок 146).

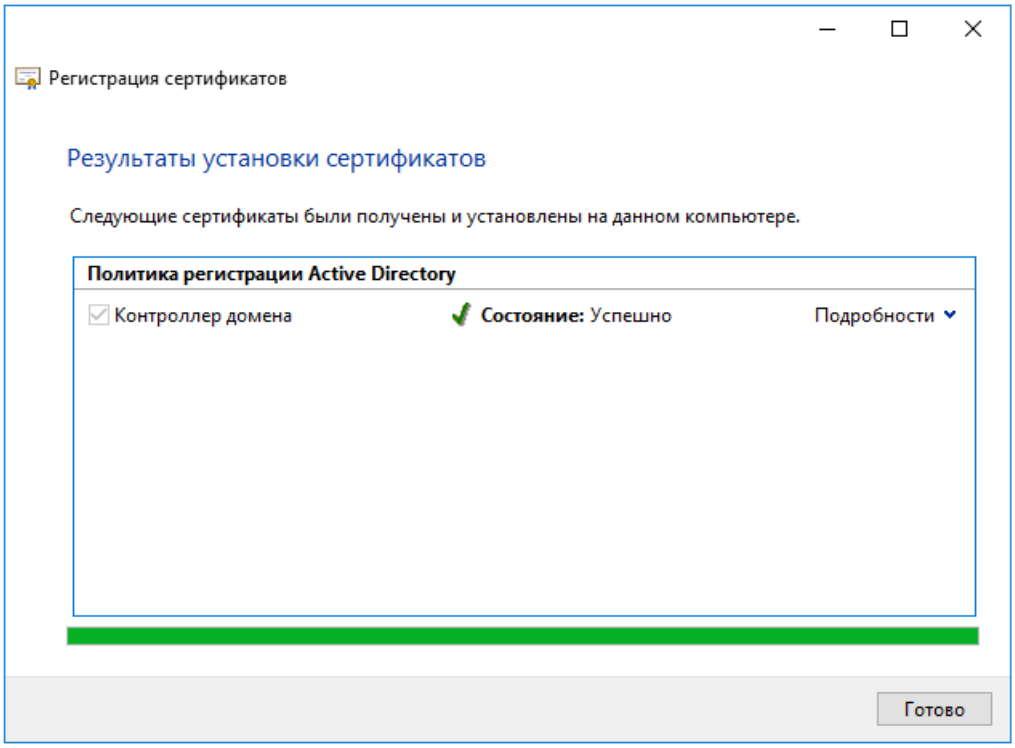


Рисунок 146. Результат установки сертификата контроллера домена

Развернув **Подробности** можно просмотреть сведения о сертификате (см. Рисунок 147).

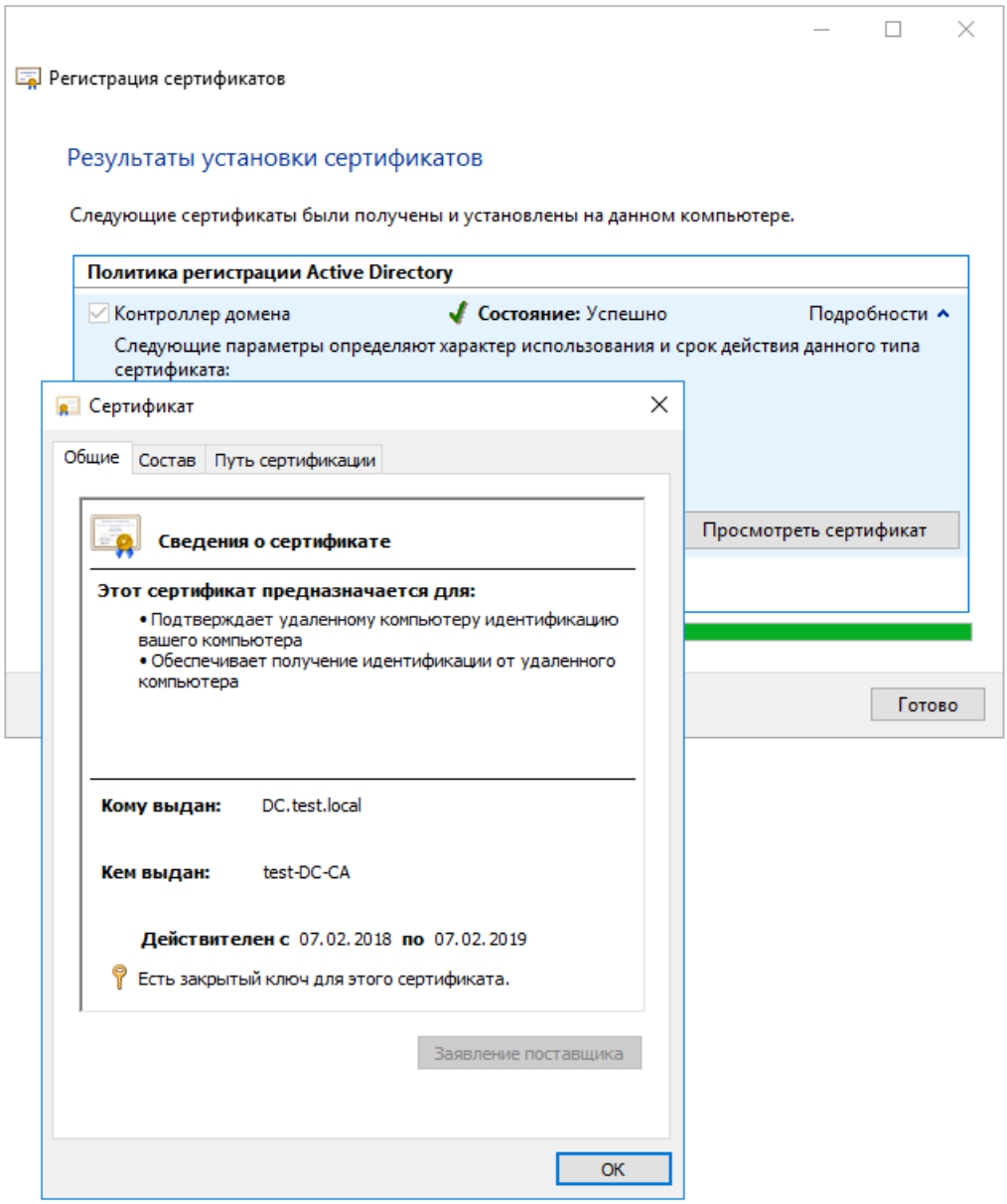


Рисунок 147. Просмотр сведений о сертификате

Сертификат контроллера домена в результате должен быть установлен в хранилище сертификатов **Личное** локального компьютера. После выпуска сертификата контроллер домена необходимо перезагрузить.

Примечание. Для сертификатов с ключами ГОСТ функции автоматического выпуска сертификатов контроллера домена недоступны, поэтому необходимо следить за действительностью сертификата и обновлять его до истечения срока действия.

5.3.1 Требования к сертификату контроллера домена

Сертификат контроллера домена должен удовлетворять следующим требованиям (подробнее см. в документации Microsoft):

• Раздел **Точка распространения списка отзыва (CRL)** должен быть заполнен и содержать путь к действительному COC, например:

Точка распределения списка отзыва (CRL)

Имя точки распространения:

Полное имя:

URL=http://server1.name.com/CertEnroll/caname.crl

• При необходимости раздел **Субъект** сертификата должен содержать уникальное имя сервера, например:
CN=Server1.northwindtraders.com
OU = Domain Controller
DC = northwindtraders
DC = com

• Раздел **Использование ключа** должен содержать:
Цифровая подпись, Шифрование ключей

• Раздел **Основные ограничения** должен содержать:
[Тип темы=Конечный субъект, Ограничение на длину пути=Отсутствует]

• Раздел **Улучшенный ключ** должен содержать:
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

• Раздел **Дополнительное имя субъекта** должен содержать DNS-имя. При использовании SMTP-репликации раздел также должен содержать глобальный уникальный идентификатор (GUID) контроллера домена в каталоге, например:
Другое имя: 1.3.6.1.4.1.311.25.1 = ac 4b 29 06 aa d6 5d 4f a9 9c 4c bc b0 6a 65 d9
DNS Name=server1.northwindtraders.com

• Шаблон сертификата должен иметь расширение со значением BMP «DomainController»

5.4 Выпуск сертификата Агента регистрации

По умолчанию разрешение на запрос сертификатов от лица пользователя предоставляется только администраторам домена. Однако пользователю, не являющемуся администратором домена, может быть предоставлено разрешение стать агентом регистрации.

Для выпуска смарт-карт агента регистрации и пользователей домена должна быть также установлена поддержка необходимых считывателей (см. разд. 2.4.1).

Примечание. Наличие сертификата агента регистрации позволяет подавать заявки на получение сертификатов и создавать смарт-карты от имени любого пользователя в составе организации. Полученная таким образом смарт-карта может затем использоваться для входа в сеть под именем пользователя без его ведома. Поскольку сертификат Агент регистрации предоставляет широкие возможности, настоятельно рекомендуется придерживаться в организации строгих политик безопасности для этих сертификатов.

Чтобы стать агентом регистрации, необходимо подать заявку на сертификат Агент регистрации через оснастку **Сертификаты – Текущий пользователь**.

Для этого через меню Пуск откройте оснастку **Сертификаты**, затем в хранилище Личное текущего пользователя выполните **Все задачи** ⇒ **Запросить новый сертификат**. В Мастере регистрации сертификатов в окне «Запрос сертификатов» из списка типов сертификатов выберите Агент регистрации и нажмите на кнопку **Свойства** (см. Рисунок 148).

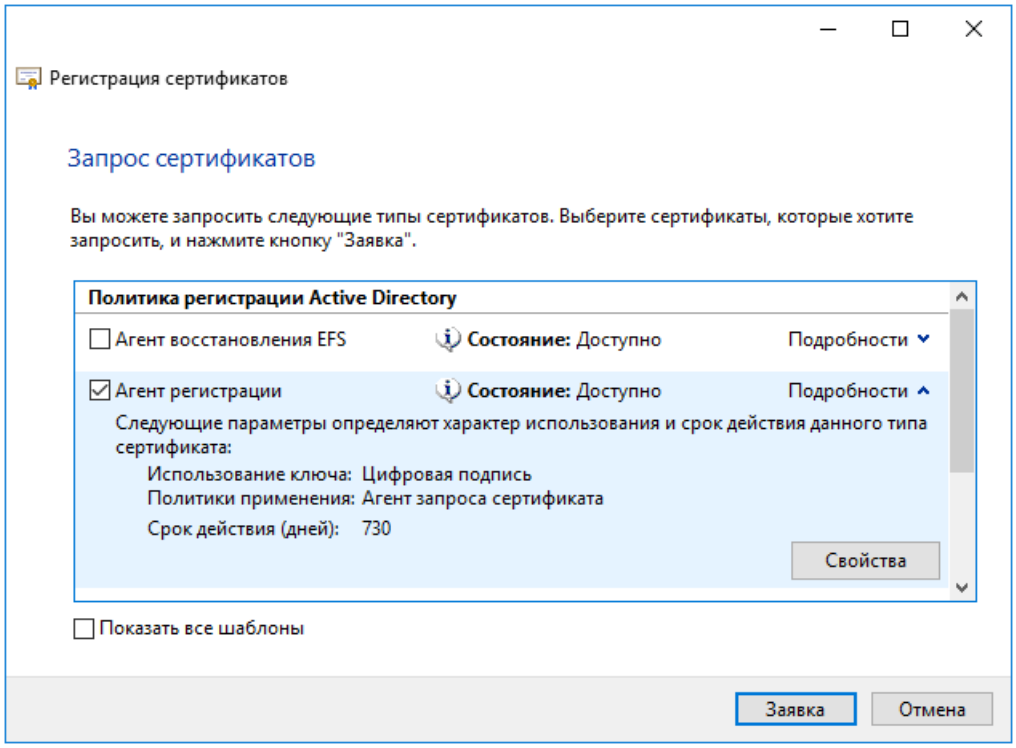


Рисунок 148. Запрос сертификата Агента регистрации

В окне «Свойства сертификата» на вкладке **Закрытый ключ** в поле **Поставщик службы шифрования** нужно указать поставщика (см. Рисунок 149). На вкладке **Центр сертификации** обязательно должен быть указан соответствующий ЦС (см. Рисунок 150).

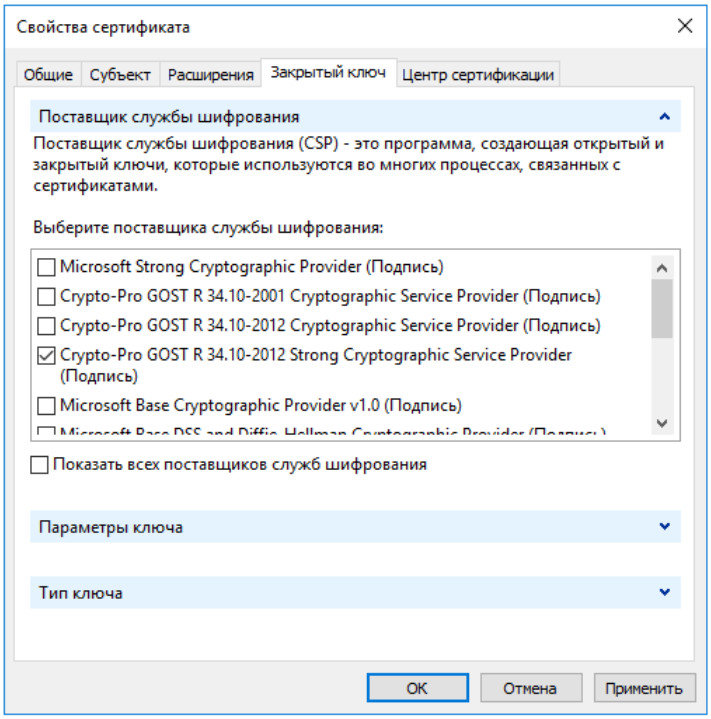


Рисунок 149. Выбор поставщика службы шифрования

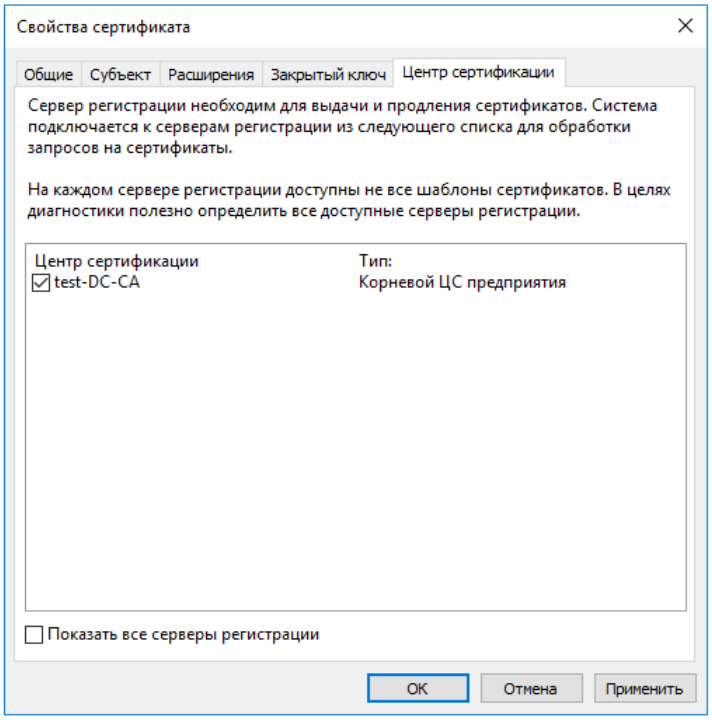


Рисунок 150. Выбор центра сертификации

После сохранения изменений нужно нажать кнопку **Заявка** для того, чтобы начать формирование контейнера с сертификатом и закрытого ключа.

Если доступно более одного считывателя, отобразится диалог выбора считывателя, в котором нужно указать, куда поместить создаваемый контейнер.

В процессе создания закрытого ключа выводится окно Биологического ДСЧ и криптопровайдер запрашивает пароль на создаваемый контейнер. После ввода пароля и выводится сообщение об успешном выпуске сертификата (см. Рисунок 151).

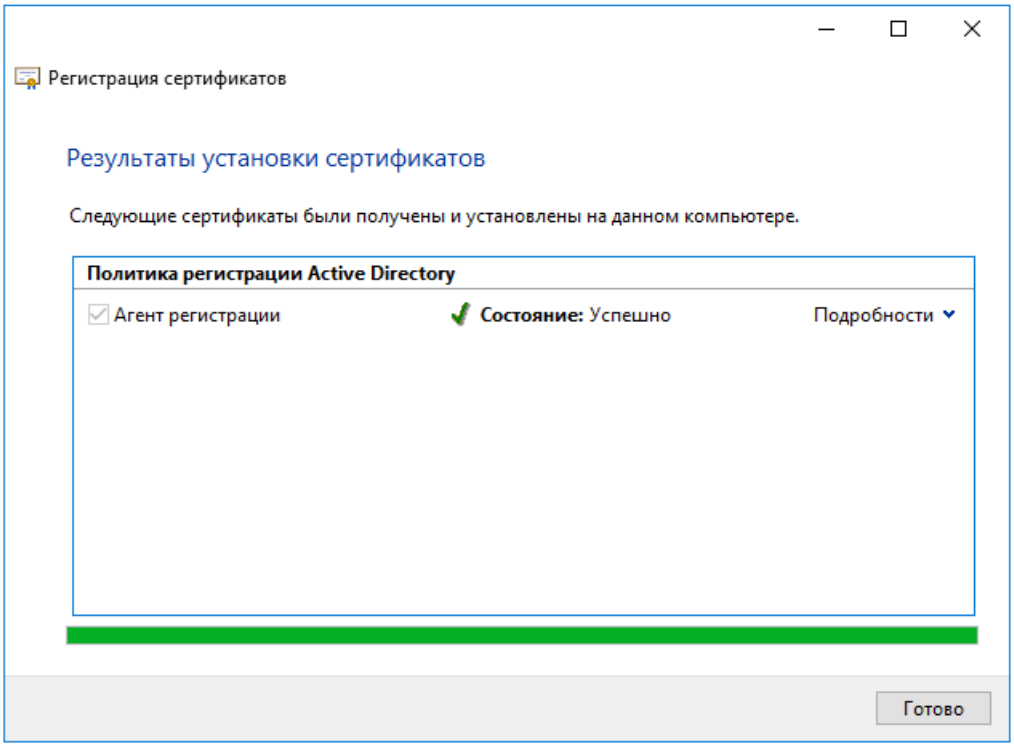


Рисунок 151. Результат установки сертификата Агента регистрации

Сертификат Агента регистрации в результате должен быть установлен в хранилище сертификатов **Личное** текущего пользователя.

5.5 Выпуск сертификатов для входа по смарт-карте

На компьютере в домене, на котором предварительно установлен КриптоПро CSP, пользователь, являющийся членом группы Пользователи и имеющий сертификат Агент регистрации, может выпускать сертификаты для других пользователей домена.

Для этого через меню Пуск откройте оснастку **Сертификаты**, затем в хранилище Личное текущего пользователя выполните **Все задачи** ⇒ **Дополнительные операции** ⇒ **Зарегистрироваться от имени** (см. Рисунок 152).

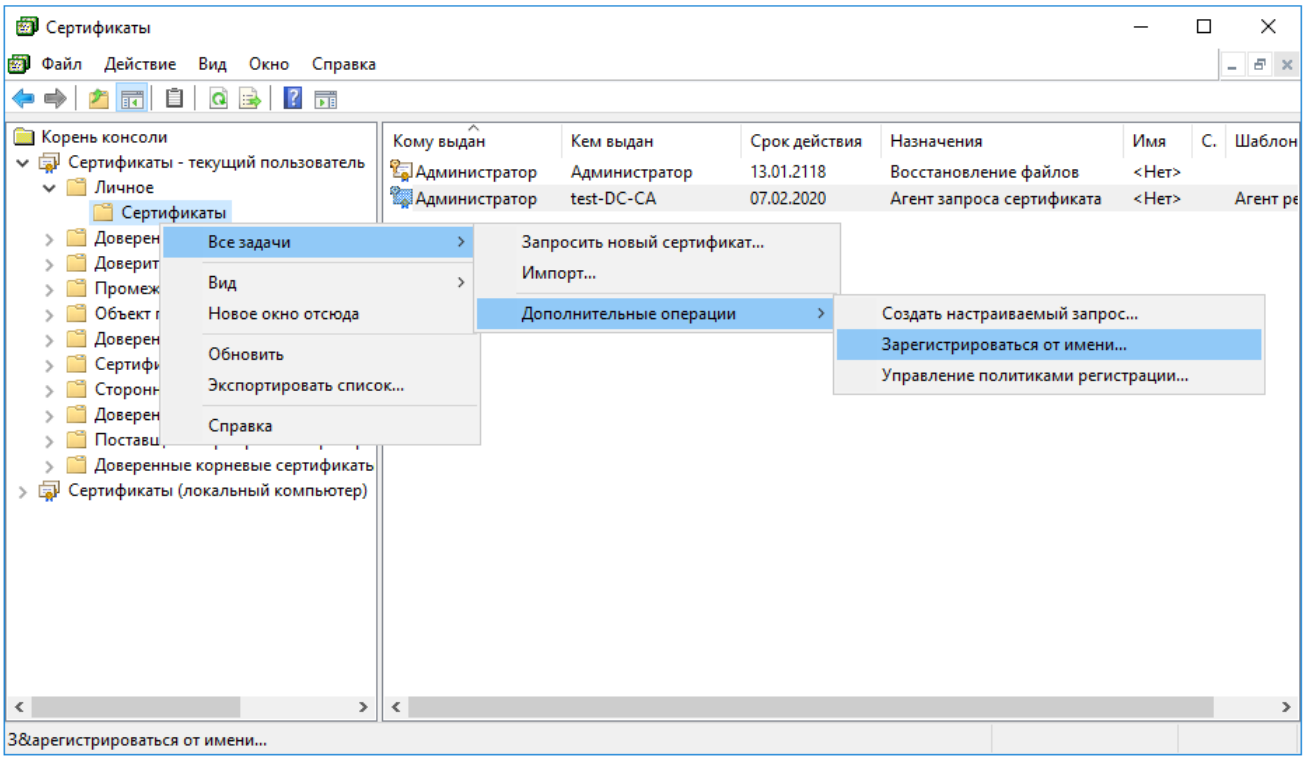


Рисунок 152. Запрос сертификата пользователя смарт-карты

В Мастере регистрации сертификатов в окне «Выберите сертификат агента регистрации» по кнопке **Обзор** выберите сертификат Агента регистрации, который будет использоваться для подписывания обрабатываемого запроса сертификата (см. Рисунок 153).

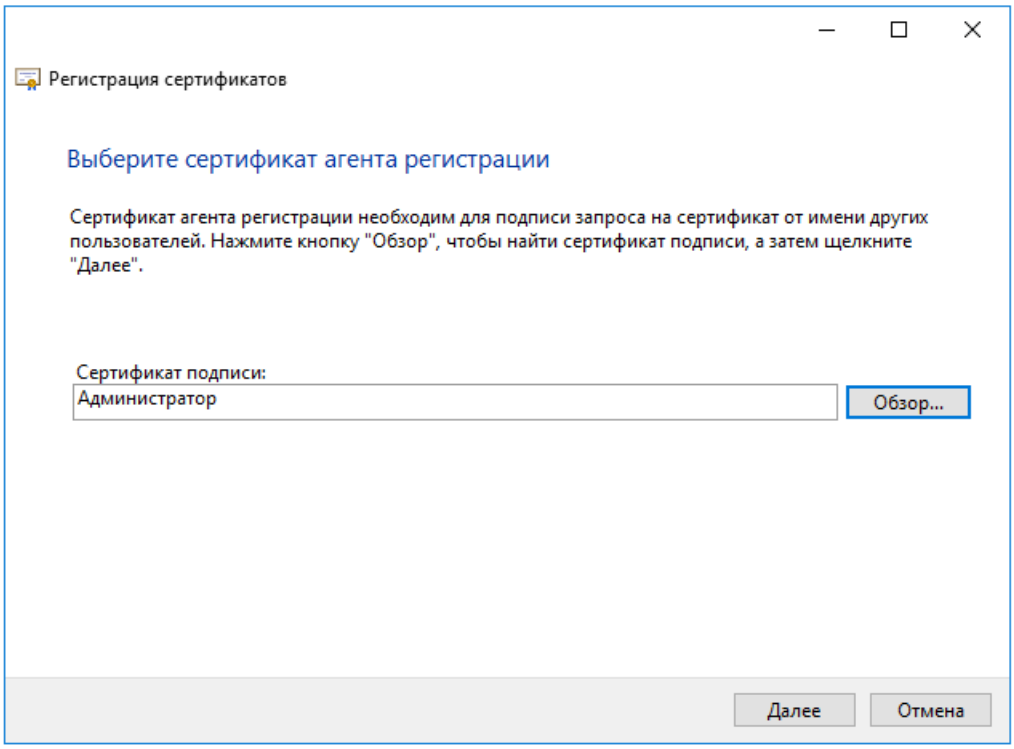


Рисунок 153. Выбор сертификата Агента регистрации

После выбора сертификата Агента регистрации из списка доступных сертификатов запрашивается пароль на доступ к этому сертификату (см. Рисунок 154).

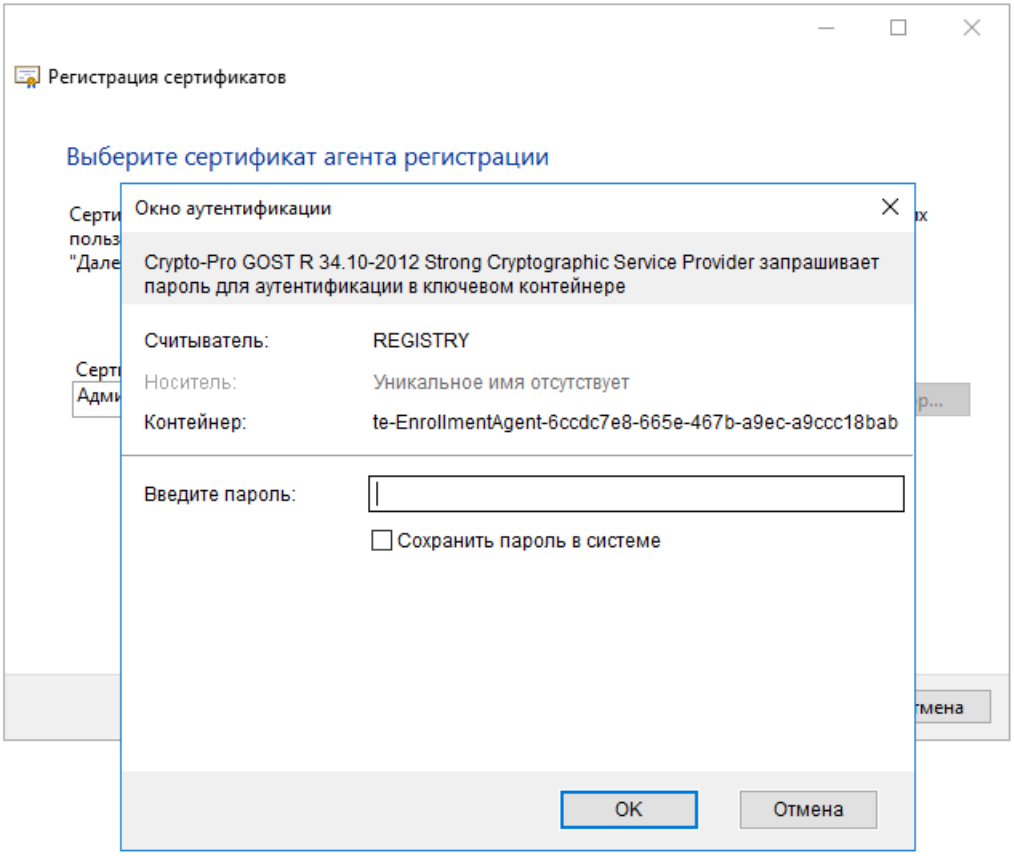


Рисунок 154. Ввод пароля для сертификата Агента регистрации

В окне «Запрос сертификатов» укажите тип сертификата **Вход со смарт-картой**. Нажмите кнопку **Свойства** для редактирования параметров выпуска сертификата (см. Рисунок 155).

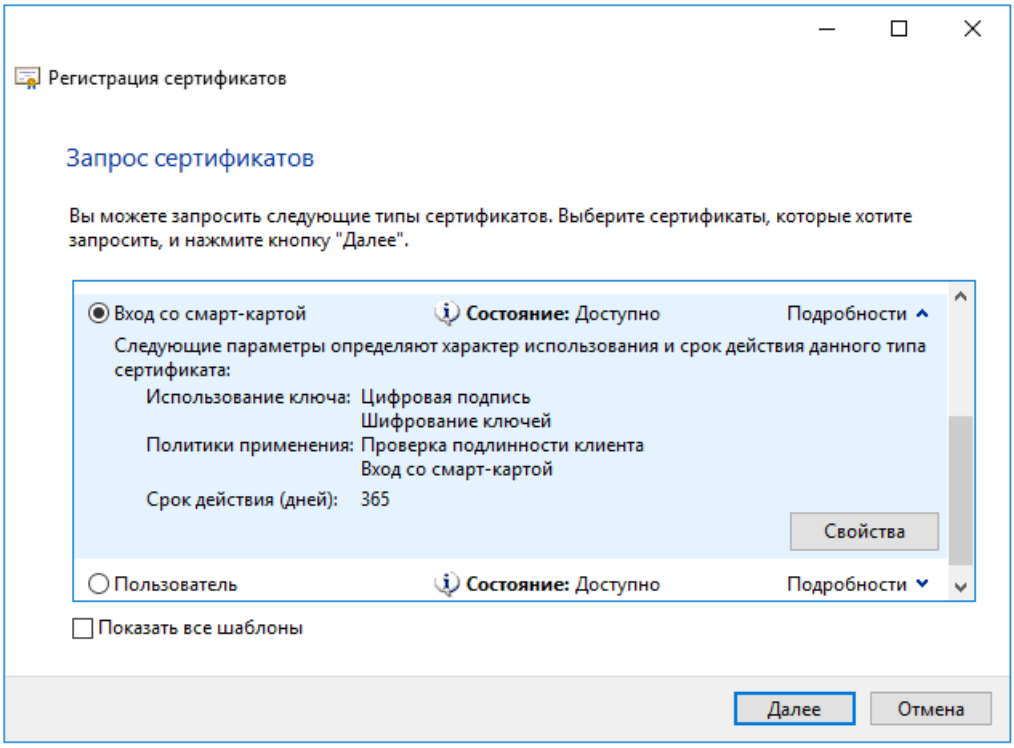


Рисунок 155. Выбор типа сертификата

Укажите поставщика службы шифрования на вкладке **Закрытый ключ** (см. Рисунок 156) и центр сертификации на вкладке **Центр сертификации** (см. Рисунок 157).

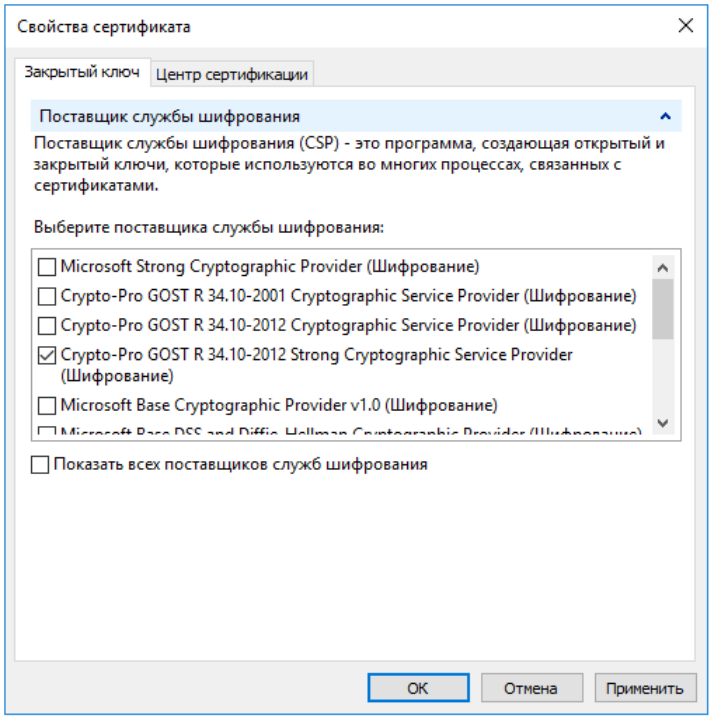


Рисунок 156. Выбор поставщика службы шифрования

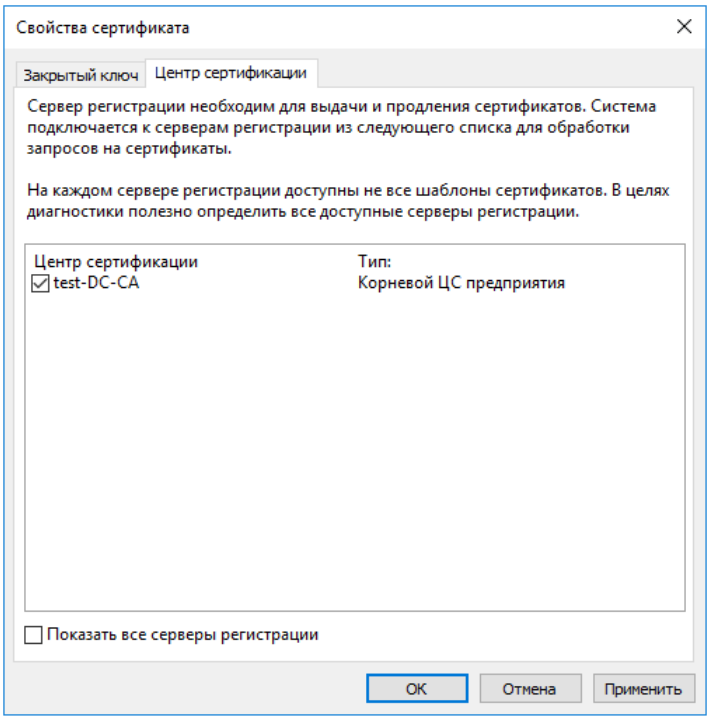


Рисунок 157. Выбор центра сертификации

Для сохранения выбранных параметров нажмите кнопку **Применить** и закройте форму. В мастере создания сертификата нажмите **Далее**, чтобы перейти к следующему шагу и выбрать пользователя домена. Выберите пользователя домена по кнопке **Обзор** и нажмите на кнопку **Заявка**, чтобы начать формирование контейнера и ключа (см. Рисунок 158).

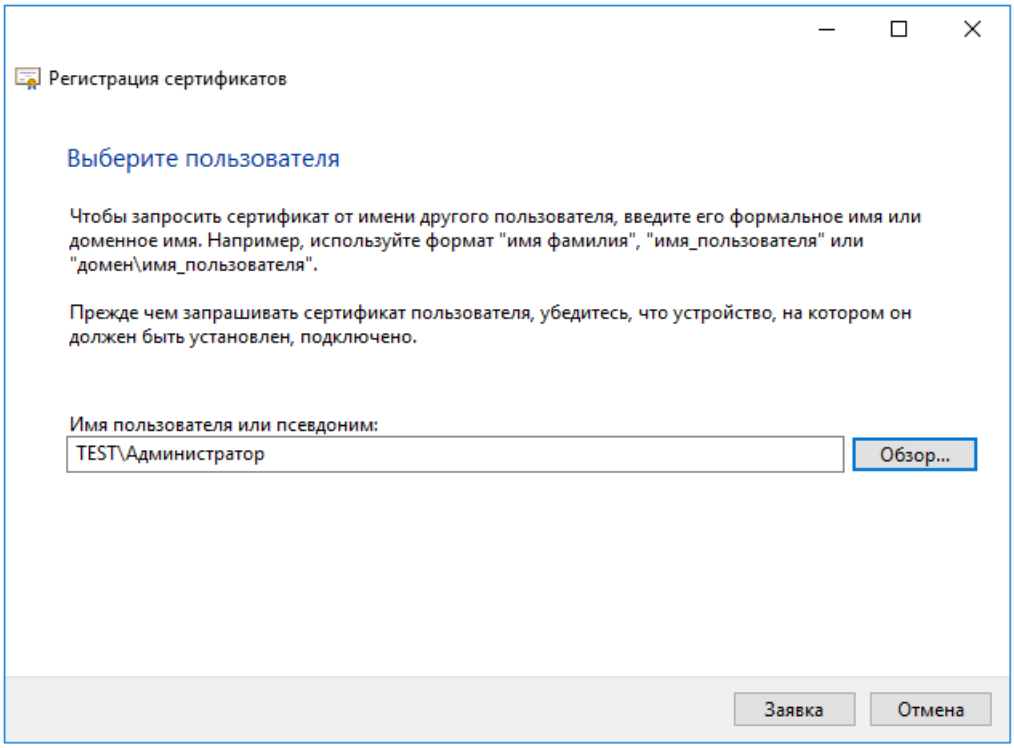


Рисунок 158. Выбор пользователя, для которого выпускается смарт-карта

Далее выбирается носитель для создания контейнера. Считыватель должен быть подключен к компьютеру, а смарт-карта определяться. В процессе формирования контейнера выводится окно Биологического ДСЧ и запрашивается пароль для нового контейнера.

В диалоге выбора пароля нужно ввести пароль для создаваемого контейнера. Для правильной работы со смарт-картой пароль для создаваемого контейнера и смарт-карты должен быть одним.

В результате выводится сообщение об успешной записи контейнера на смарт-карту (см. Рисунок 159).

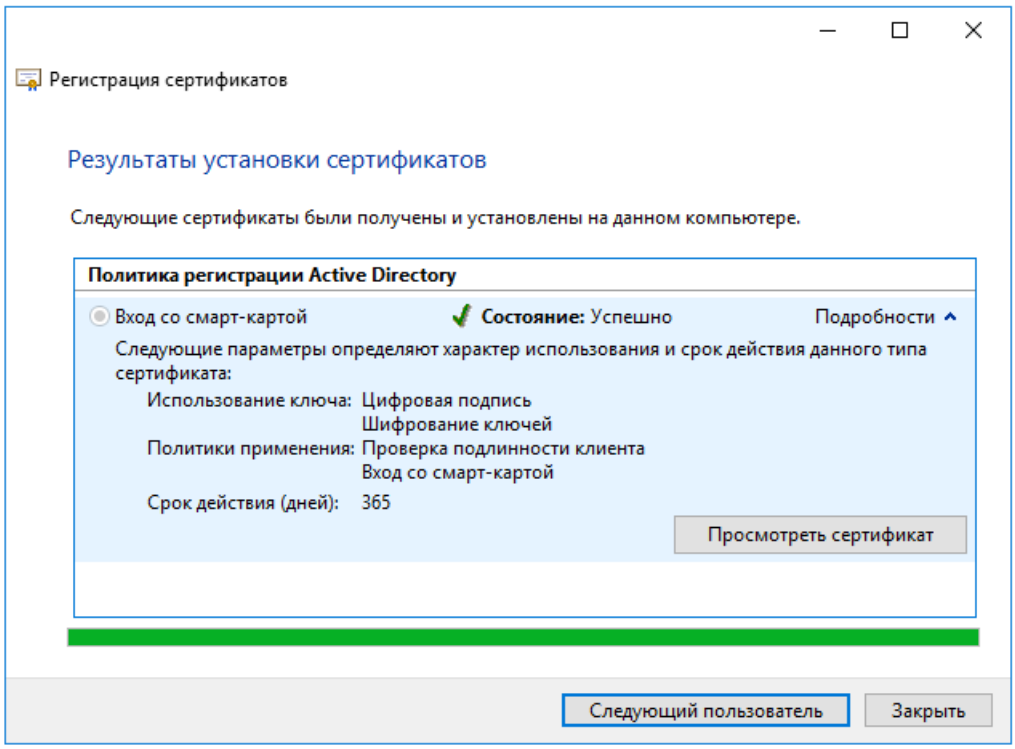


Рисунок 159. Результат выпуска сертификата

После того, как контейнер записан на носитель, вход с доменной учетной записью пользователя может осуществляться с авторизацией по смарт-карте.

Для авторизации пользователя домена к компьютеру, с которого осуществляется вход в домен, нужно подключить считыватель и вставить в него смарт-карту, затем из параметров входа выбрать значок «Смарт-карта» и ввести ПИН-код (см. Рисунок 160).

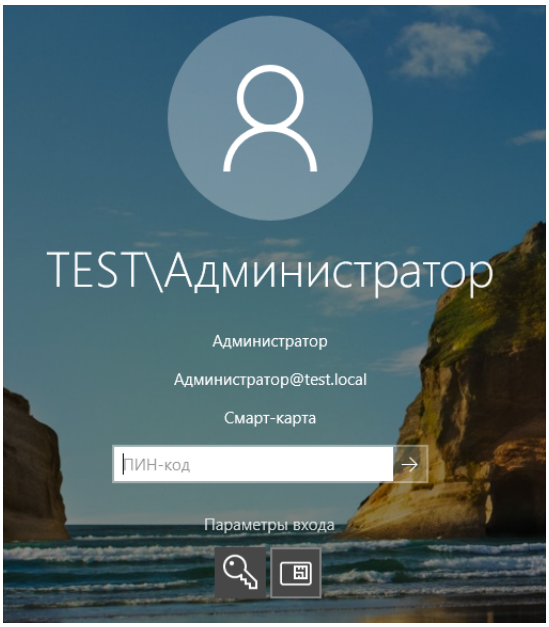


Рисунок 160. Авторизация с помощью смарт-карты пользователя домена

5.5.1 Требования к сертификату для входа по смарт-карте

Сертификат для входа по смарт-карте должен удовлетворять следующим требованиям (подробнее см. в документации Microsoft):

• Раздел **Точка распространения списка отзыва (CRL)** должен быть заполнен и содержать путь к действительному COC, например:

[1]Точка распределения списка отзыва (CRL)
Имя точки распространения:
Полное имя:
URL=http://server1.name.com/CertEnroll/caname.crl

• Раздел **Использование ключа** должен содержать:

Цифровая подпись

• Раздел **Основные ограничения** должен содержать:

[Тип темы=Конечный субъект, Ограничение на длину пути=Отсутствует] (Необязательно)

• Раздел **Улучшенный ключ** должен содержать:

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
(Проверка подлинности клиента требуется только в случаях, когда сертификат используется для проверки подлинности по протоколу SSL)
Вход в систему с помощью смарт-карты (1.3.6.1.4.1.311.20.2.2)

• Раздел **Дополнительное имя субъекта** должен содержать значение вида Другое имя: Имя субъекта = (UPN). Например:

Другое имя:
Имя субъекта = user@test.local

• Раздел **Субъект** должен содержать уникальное имя пользователя, например:

CN = User
CN = Users
DC = test
DC = local

5.6 Настройка Active Directory и контроллера домена для входа по смарт-картам с помощью групповой политики при использовании стороннего центра сертификации

Для проверки подлинности с помощью смарт-карты в Active Directory необходимо, чтобы рабочие станции со смарт-картами, Active Directory и контроллеры доменов Active Directory были правильно настроены. Чтобы выполнить проверку подлинности пользователей на основе сертификатов от центра сертификации, нужно, чтобы приложение Active Directory доверяло этому центру сертификации. Рабочие станции со смарт-картами, и контроллеры доменов должны быть настроены с правильно настроенными сертификатами.

При любой реализации инфраструктуры открытого ключа (PKI) необходимо, чтобы все участники доверяли корневому центру сертификации, к которому привязывается выпускающий центр сертификации. И контроллеры доменов, и рабочие станции со смарт-картами доверяют этому корневому центру.

Для настройки Active Directory и контроллера домена необходимы следующие условия:

- Для выполнения проверки подлинности пользователей в Active Directory сторонние выпускающие центры сертификации должны находиться в хранилище NTAuth.
- Для выполнения проверки подлинности пользователей с помощью смарт-карт контроллеры доменов должны быть настроены с сертификатом контроллера домена.
- Также можно настроить Active Directory так, чтобы независимые корневые центры сертификации распространялись в хранилища доверенных корневых центров сертификации всех членов домена с помощью групповой политики.

5.6.1 Указания по настройке

Для настройки необходимо иметь независимый корневой сертификат в кодировке Base64 X.509, а также сертификаты выпускающих ЦС.

5.6.1.1 Добавление независимого корневого центра сертификации к доверенным корневым центрам в объект групповой политики службы Active Directory

Настройка групповой политики в домене Windows для распространения независимых корневых центров сертификации в хранилища доверенных корневых центров всех компьютеров домена производится следующим образом:

1) Откройте в консоли mmc оснастку **Управление групповой политикой**.

2) Разверните в открывшейся оснастке элементы: **Управление групповой политикой** ⇒ **Лес: <имя домена>** ⇒ **Домены**. На соответствующем домене выберите в контекстном меню **Изменить** (см. Рисунок 161).

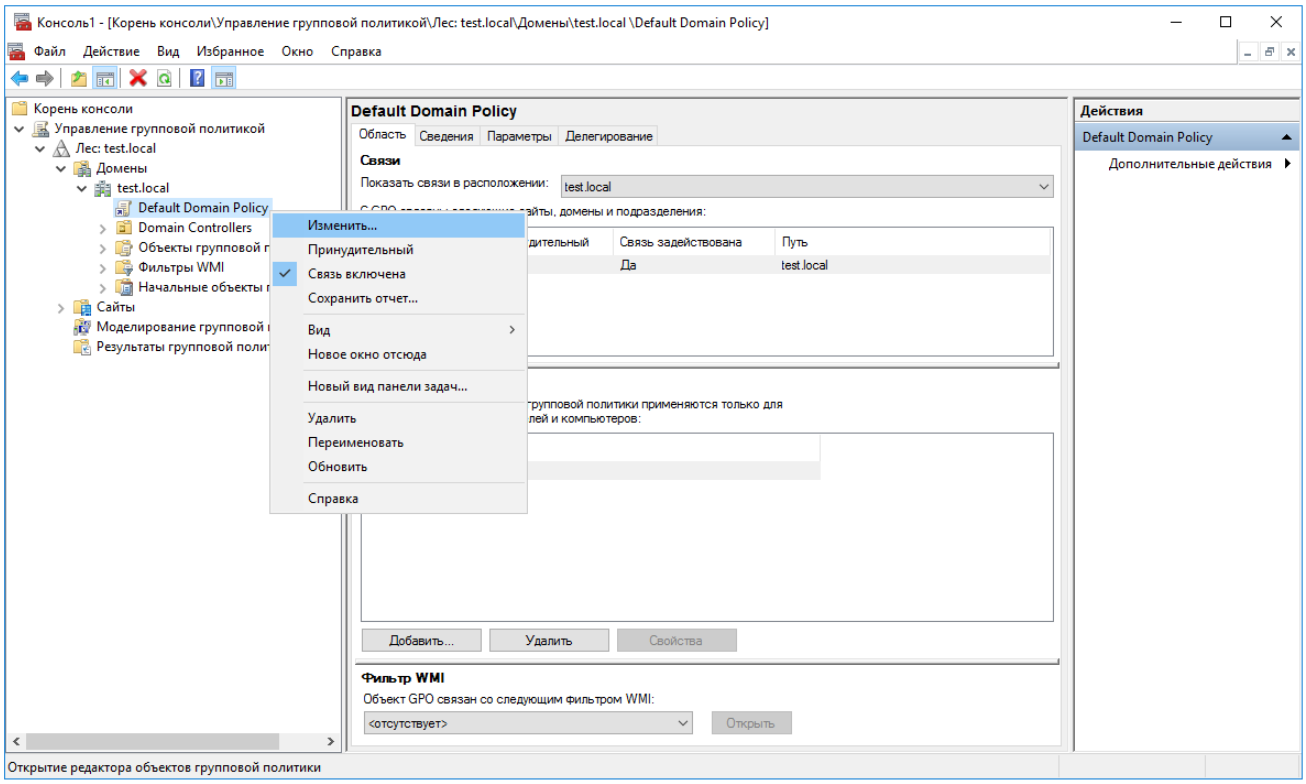


Рисунок 161. Оснастка Управление групповой политикой

3) В редакторе управления групповыми политиками разверните **Конфигурация компьютера** ⇒ **Политики** ⇒ **Конфигурация Windows** ⇒ **Параметры безопасности** ⇒ **Политики открытого ключа** ⇒ **Доверенные корневые центры сертификации** (см. Рисунок 162). В это хранилище импортируйте корневой сертификат ЦС, открыв через контекстное меню мастер импорта сертификатов и следуя указаниям мастера.

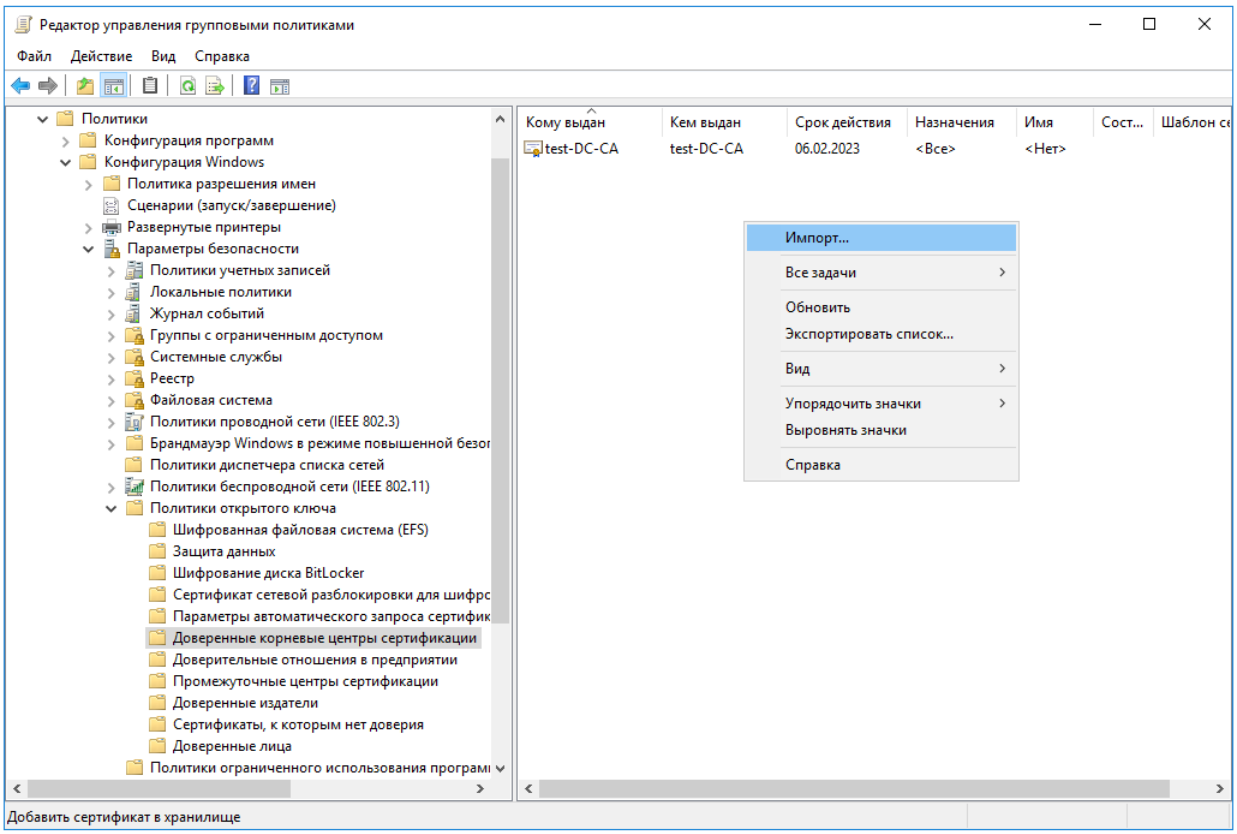


Рисунок 162. Добавление сертификата доверенного УЦ в групповые политики

5.6.1.2 Добавление сторонних выпускающих центров сертификации в хранилище NTAuth службы Active Directory

Сертификат входа по смарт-карте должен быть выпущен центром сертификации, находящимся в хранилище NTAuth. Корневые сертификаты центров сертификации Microsoft Enterprise CA автоматически добавляются в хранилище NTAuth, а сертификаты сторонних центров сертификации необходимо поместить в хранилище вручную или с помощью утилиты certutil, которая присутствует в поставке Microsoft Windows.

Хранилище NTAuth для всего леса находится в контейнере конфигурации. Примерное расположение: `LDAP://server1.name.com/CN=NTAuthCertificates,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=name,DC=com`

По умолчанию это хранилище создается при установке центра сертификации Microsoft Enterprise.

Для того, чтобы поместить сертификат в хранилище NTAuth с помощью certutil сохраните его в файл и выполните следующую команду:

`certutil -dspublish -f <filename> NTAuthCA`, где <filename> – имя файла с сертификатом.

После помещения сертификатов независимого центра сертификации в хранилище NTAuth групповая политика на базе домена размещает раздел реестра (отпечаток сертификата) на всех компьютерах домена в следующем разделе: `HKEY_LOCAL_MACHINE\Software\Microsoft\EnterpriseCertificates\NTAuth\Certificates`.

Обновление на рабочих станциях происходит каждые восемь часов (стандартный интервал групповой политики). При необходимости можно принудительно применить групповую политику с помощью команды на сервере `gpupdate/force`.

5.6.1.3 Запрос и установка сертификата контроллеров домена на контроллер(ы) домена

Каждый контроллер домена, выполняющий проверку подлинности пользователей по смарт-картам, должен иметь сертификат контроллера домена. При установке центра сертификации Microsoft Enterprise в лес службы Active Directory все контроллеры домена отмечаются в сертификате контроллеров домена автоматически. Формат сертификата должен отвечать требованиям к сертификату контроллера домена (см. разд. 5.3.1).

Подробно запрос и установка сертификата рассматриваются в разделе Выпуск сертификата контроллера домена.

6 Использование КриптоПро CSP при работе с почтовым клиентом The Bat!

Для защиты переписки через электронную почту по стандарту протокола S/MIME в почтовом клиенте The Bat! с использованием ГОСТ-алгоритмов при шифровании и подписывании сообщений нужно выполнить ряд настроек:

1) указать параметры S/MIME в настройках почтового клиента;
2) настроить почтовый ящик;
3) обменяться сертификатами с другими участниками переписки и поместить их в хранилища сертификатов.

Предварительно на компьютере пользователя должно быть установлено СКЗИ КриптоПро CSP.

6.1 Настройка параметров S/MIME почтового клиента

Для настройки параметров S/MIME почтового клиента в главном меню The Bat! выберите **Свойства – S/MIME и TLS...**. Откроется окно «Параметры S/MIME и TLS» (см. Рисунок 163).

Укажите следующие настройки S/MIME и TLS:

- в блоке **Реализация S/MIME и сертификаты TLS** выберите **Microsoft CryptoAPI**;
- установите флаг **Всегда шифровать отправителю**, если необходимо, чтобы исходящая почта шифровалась с помощью сертификата получателя в случае, если такой сертификат есть;
- в поле **Криптопровайдер** выберите из выпадающего списка поставщика служб шифрования;
- установите флаг **Никогда не использовать других криптопровайдеров**, если данный почтовый клиент не планируется использовать с другими поставщиками служб шифрования;
- в поле **Алгоритм шифрования** укажите алгоритм шифрования, соответствующий выбранному криптопровайдеру;
- в поле **Хэш-алгоритм подписи** укажите хэш-алгоритм подписи;
- установите флаг **Помнить связи e-mail адресов с сертификатами для подписи** для автоматического выбора соответствующих используемому e-mail адресу сертификатов для подписи;
- установите флаг **Помнить связи e-mail адресов с сертификатами для шифрования** для автоматического выбора соответствующих используемому e-mail адресу сертификатов для шифрования;

Сохраните настройки, нажав кнопку **OK**.

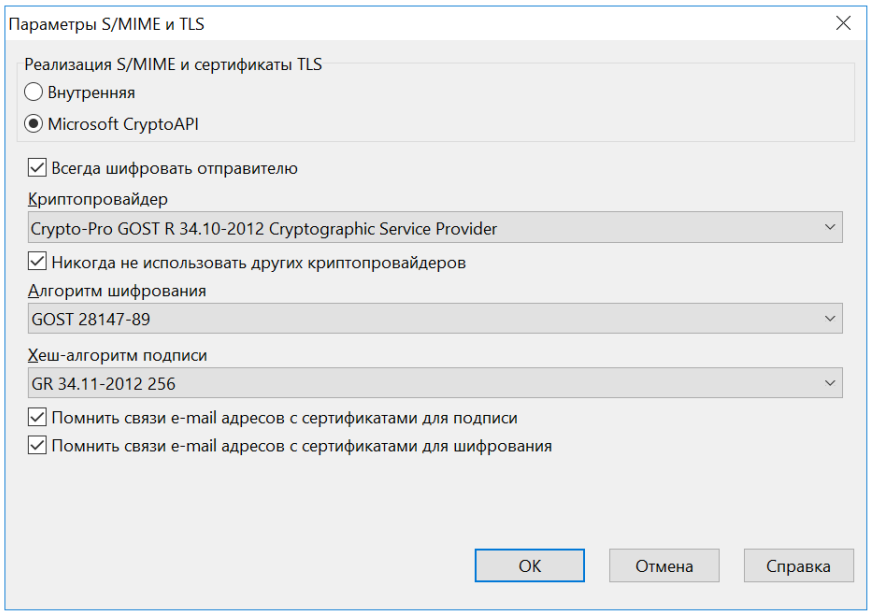


Рисунок 163. Настройка параметров S/MIME и TLS

6.2 Настройка почтового ящика

Для настройки параметров почтового ящика выделите почтовый ящик и в главном меню The Bat! выберите **Ящик – Свойства почтового ящика...**. В открывшемся окне «Свойства» почтового ящика выберите раздел **Параметры**. (см. Рисунок 164).

В секции **Редактор писем** установите флаг **Авто-S/MIME**. Также можно включить опции **Подписать перед отправкой** и **Зашифровать перед отправкой**.

Сохраните настройки, нажав кнопку **OK**.

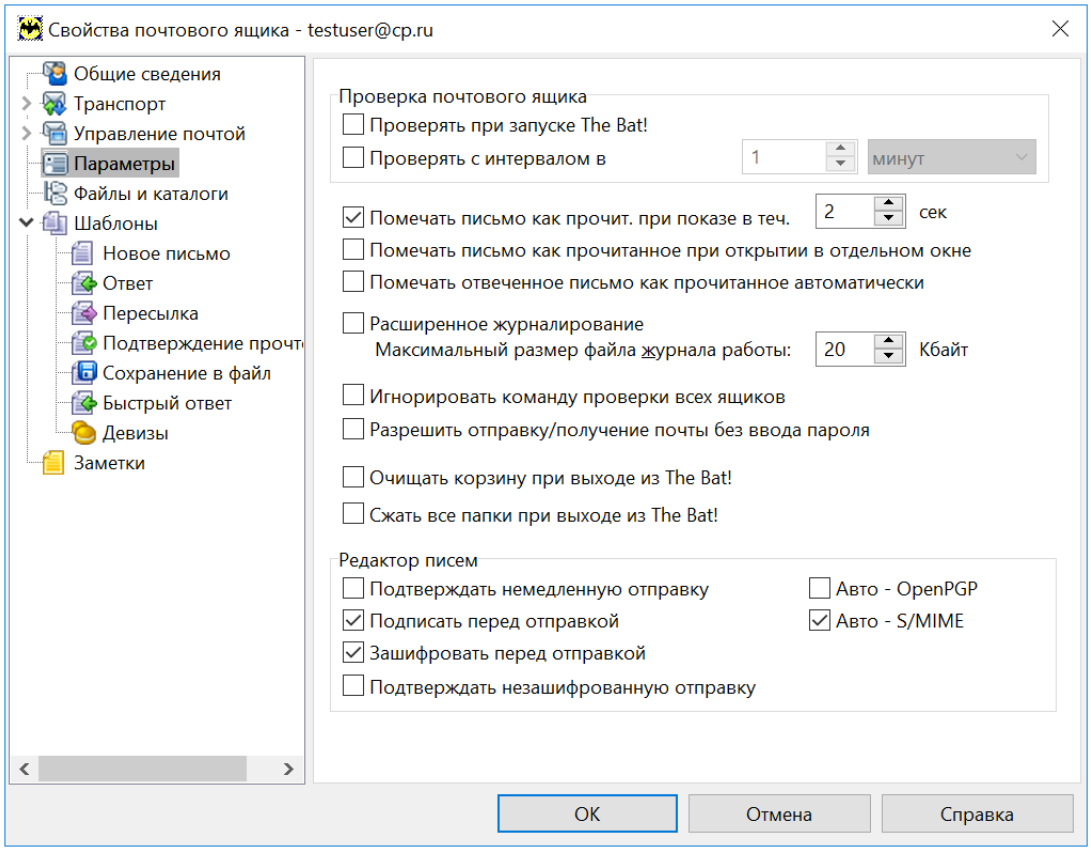


Рисунок 164. Редактирование свойств почтового ящика

Примечание. В почтовом клиенте The Bat! возможно настроить только один почтовый ящик, работающий с электронной подписью и шифрованием писем.

6.3 Обмен сертификатами

Для того, чтобы подписывать письма и шифровать их в адрес получателя при отправке с помощью почтового клиента, в хранилищах сертификатов компьютера должны находиться сертификат отправителя с ключом и сертификаты получателей. Сертификат отправителя с ключом также может храниться на съемном носителе (смарт-карте, USB-токене и тд.), который должен быть подключен к компьютеру при работе с почтой — он содержит сведения об электронном адресе, для работы с которым он был выпущен.

При наличии сертификата с ключом пользователь может подписывать письма электронной подписью, но для того, чтобы зашифровать сообщение, необходимо, чтобы в хранилище сертификатов отправителя находился сертификат получателя, содержащий открытый ключ.

Самый простой способ установить сертификат в нужное хранилище — получить письмо, которое содержит

электронную подпись, и добавить отправителя в адресную книгу.

Для этого необходимо выполнить следующие действия:

1) При просмотре подписанного письма нажмите кнопку **Просмотреть действительную подпись** (см. Рисунок 165).

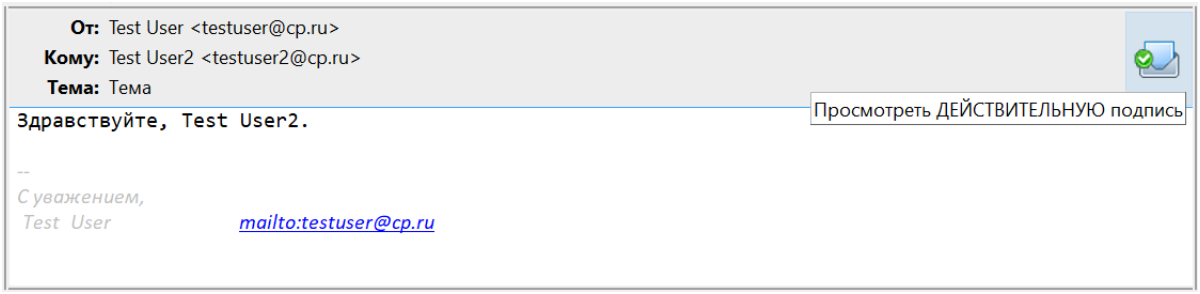


Рисунок 165. Функция просмотра подписи в The Bat!

2) В окне проверки подписи нажмите кнопку **Просмотреть свойства сертификата** (см. Рисунок 166).

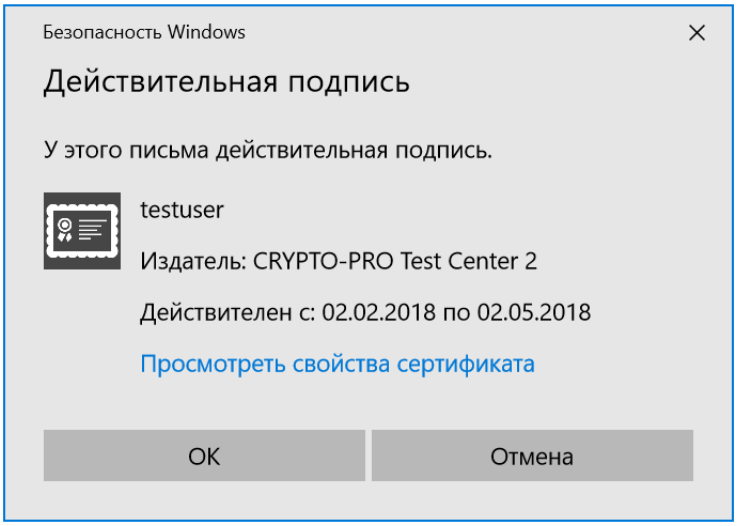


Рисунок 166. Окно просмотра подписи

3) В окне просмотра свойств сертификата нажмите кнопку **Установить сертификат** (см. Рисунок 167).

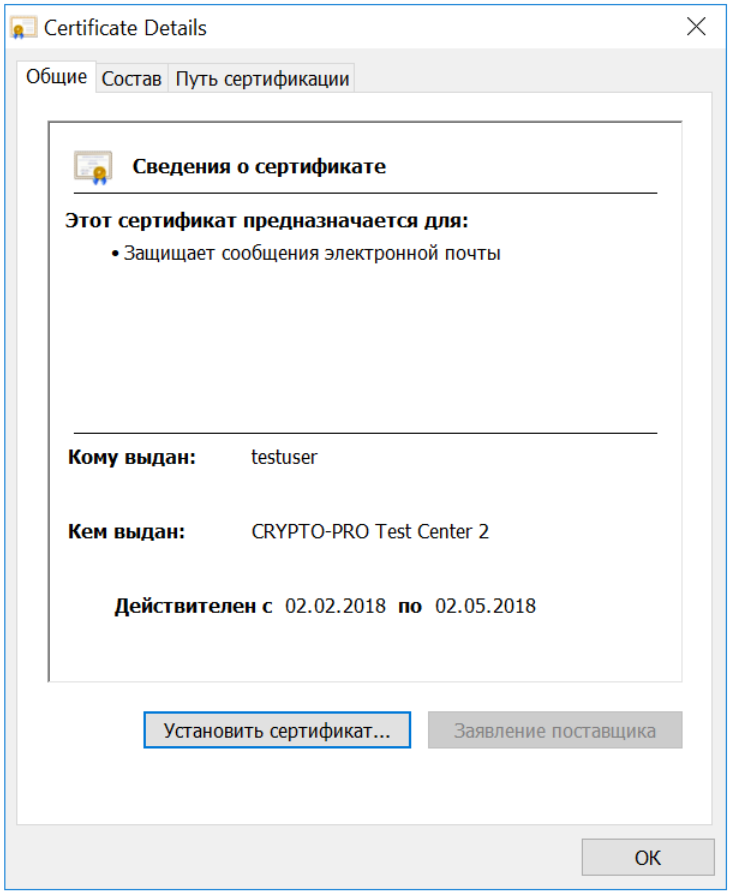


Рисунок 167. Форма просмотра сертификата

4) В открывшемся Мастере импорта сертификатов выберите хранилище Текущего пользователя и нажмите кнопку **Далее** (см. Рисунок 168).

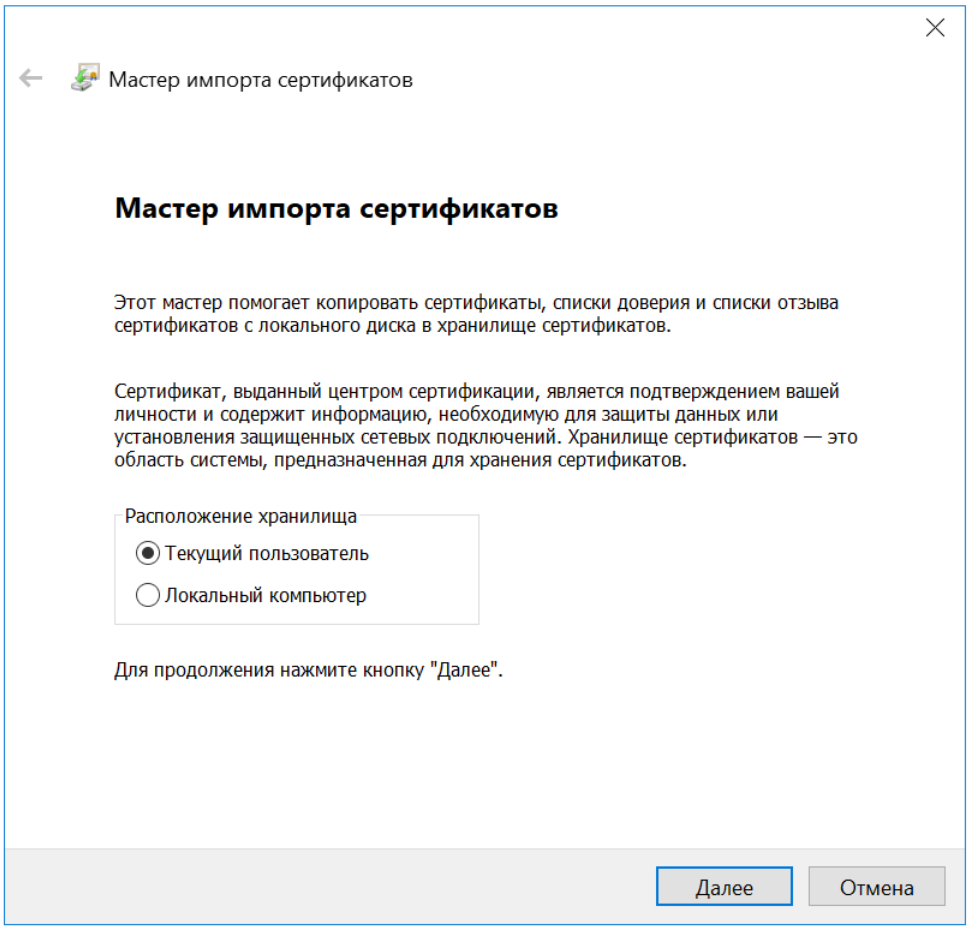


Рисунок 168. Выбор расположения хранилища при импорте сертификата

5) На следующем шаге с помощью кнопки **Обзор** выберите хранилище Другие пользователи и нажмите кнопку **Далее** (см. Рисунок 169).

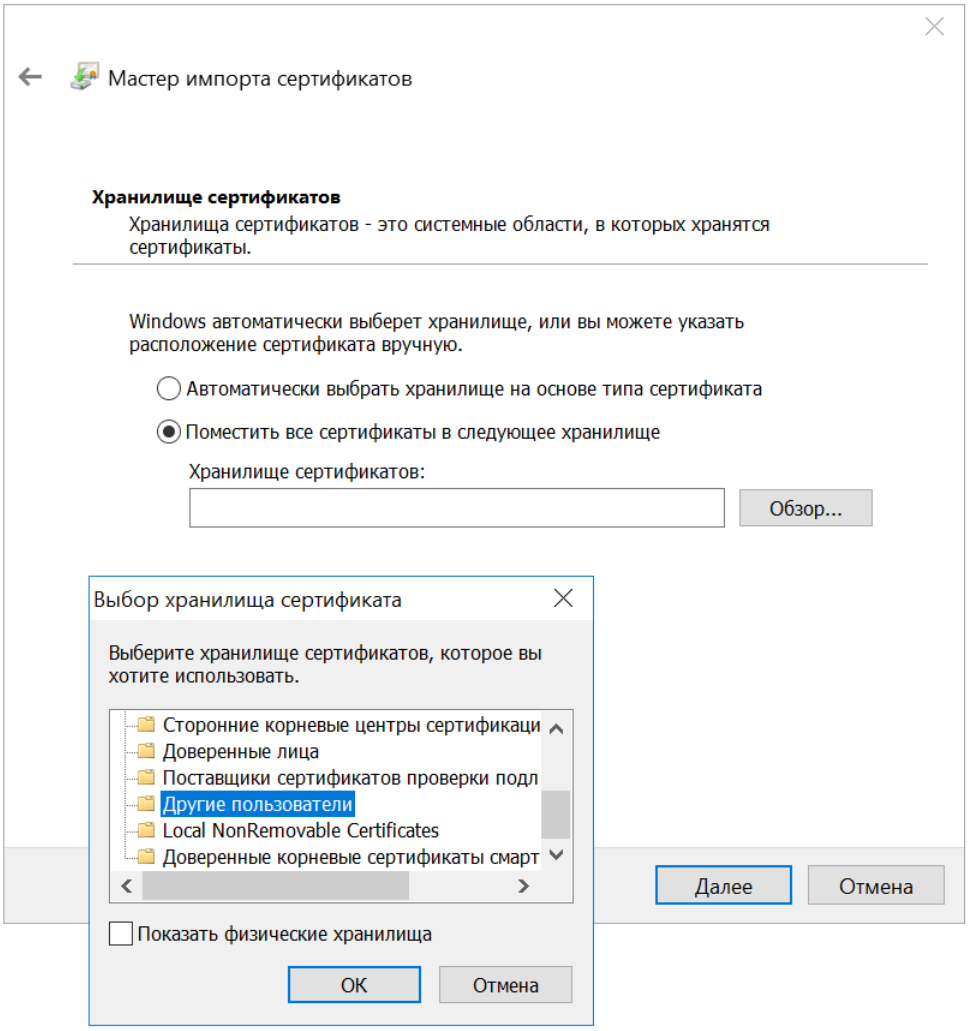


Рисунок 169. Выбор хранилища при импорте сертификата

6) По завершении работы мастера нажмите кнопку **Готово**. Появится сообщение об успешном выполнении импорта.

После этого в адрес владельца сертификата можно отправлять зашифрованные письма,

6.4 Отправка зашифрованных сообщений

Для создания и отправки зашифрованного сообщения нажмите на кнопку **Создать новое письмо**.

Для того, чтобы зашифровать сообщение, нажмите на кнопку **Зашифровать перед отправкой** на панели Безопасность в окне редактирования письма (см. Рисунок 170).

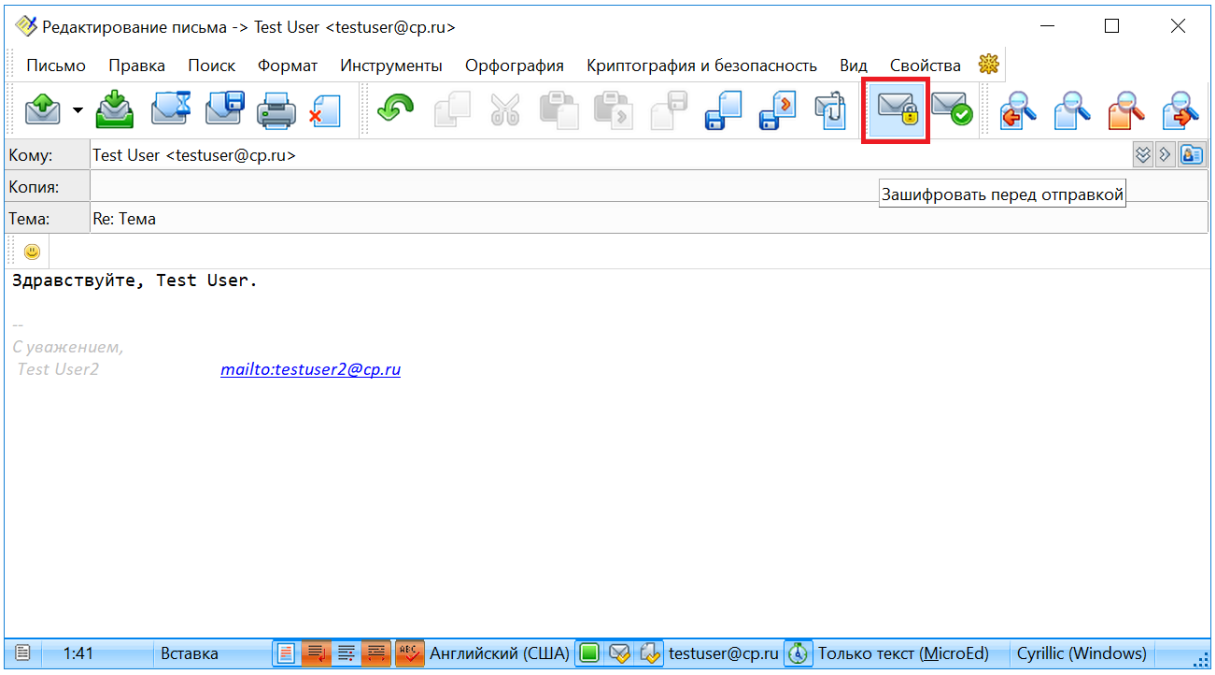


Рисунок 170. Функция шифрования в форме редактирования письма

Для отправки сообщения нажмите кнопку **Отправить письмо**. В открывшемся окне выберите сертификат получателя для шифрования письма (см. Рисунок 171).

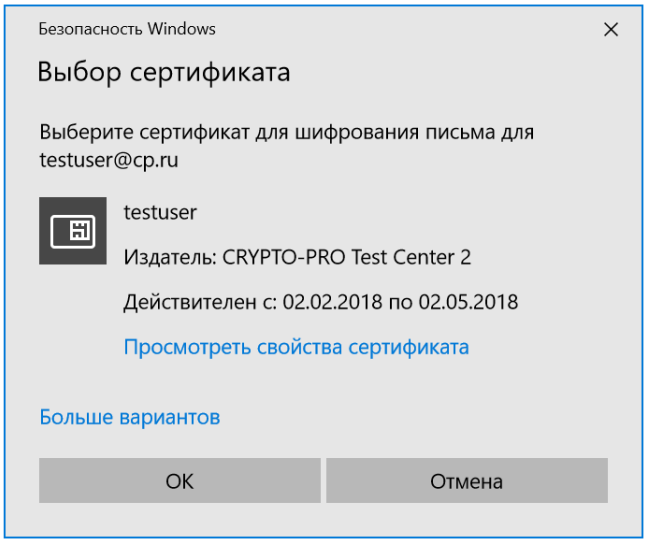


Рисунок 171. Выбор сертификата для шифрования письма

Если при попытке зашифровать письмо не удалось найти сертификат получателя, появится следующее предупреждение (см. Рисунок 172).

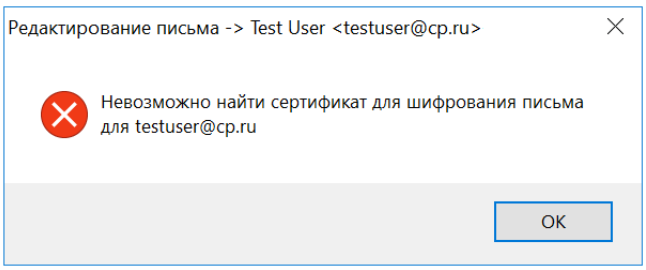


Рисунок 172. Ошибка при шифровании письма

6.5 Просмотр зашифрованных сообщений

Просмотр зашифрованных сообщений доступен только пользователям, у которых установлен сертификат, который использовался отправителем при шифровании сообщения.

В области предварительного просмотра письма текст зашифрованного сообщения не отображается. Для просмотра текста зашифрованного сообщения нажмите кнопку **Расшифровать письмо S/MIME** (см. Рисунок 173).

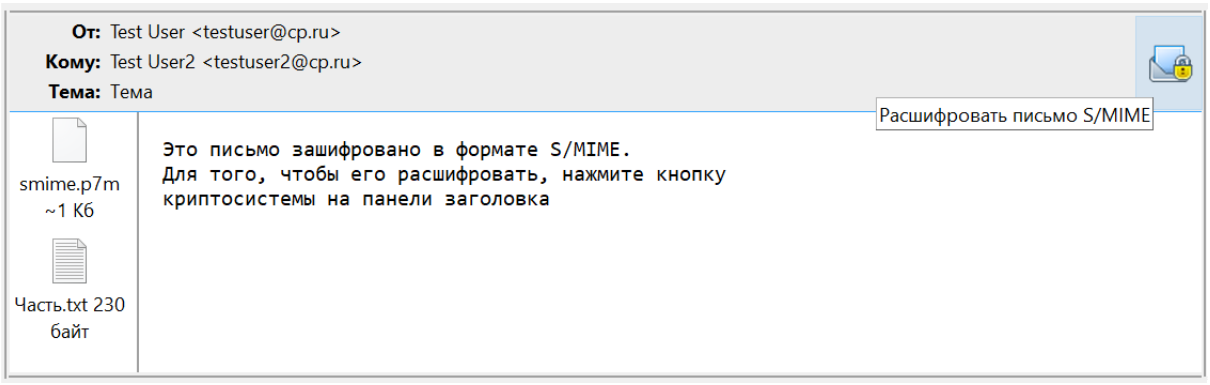


Рисунок 173. Просмотр зашифрованного письма

Если на доступ к закрытому ключу установлен пароль, откроется окно аутентификации в ключевом контейнере. Введите пароль на доступ к контейнеру и нажмите кнопку **OK**.

В случае корректного расшифрования сообщения откроется закладка Текст с исходным текстом письма.

Если у получателя зашифрованного письма отсутствует сертификат, который использовался при шифровании данного сообщения, при нажатии на кнопку **Расшифровать письмо S/MIME** откроется окно с ошибкой (см. Рисунок 174).

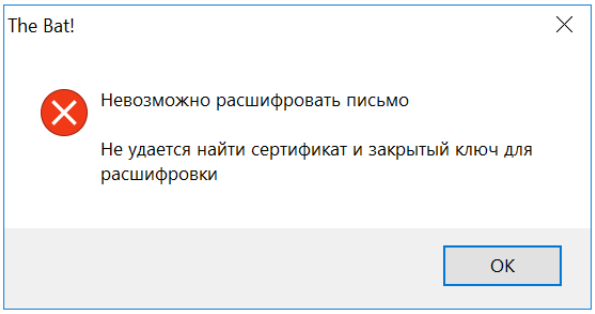


Рисунок 174. Ошибка при расшифровании письма

6.6 Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите на кнопку **Создать новое письмо**.

Для того, чтобы подписать сообщение, нажмите на кнопку **Подписать перед отправкой** на панели Безопасность в окне редактирования письма (см. Рисунок 175).

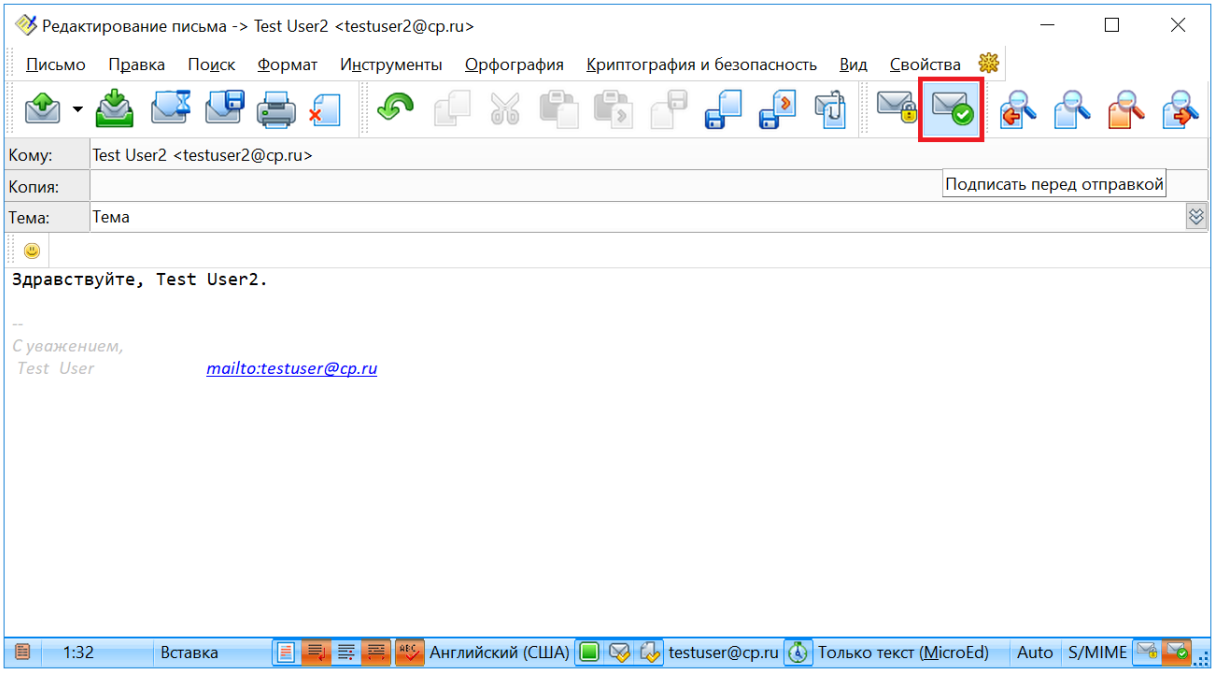


Рисунок 175. Функция подписи в форме редактирования письма

Для отправки сообщения нажмите кнопку **Отправить письмо**. В открывшемся окне выберите сертификат для подписи письма (см. Рисунок 176).

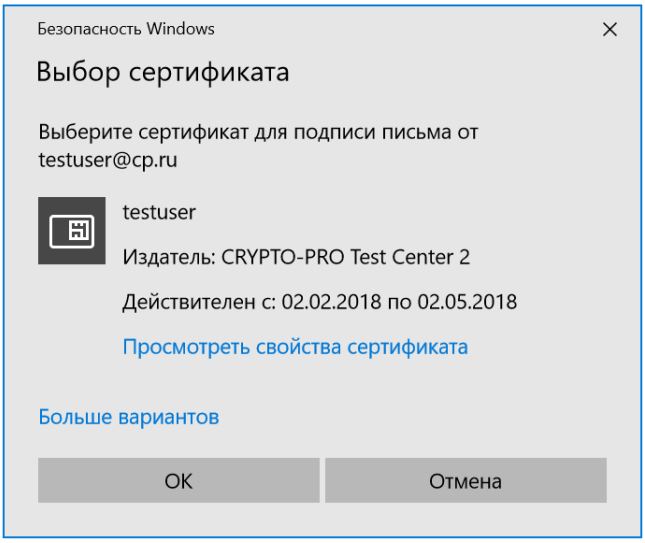


Рисунок 176. Окно выбора сертификата для подписи

Если на доступ к закрытому ключу установлен пароль, откроется окно аутентификации в ключевом контейнере. Введите пароль на доступ к контейнеру и нажмите кнопку **OK**.

Если у пользователя отсутствует подходящий сертификат для подписи сообщений, откроется окно с ошибкой (см.

Рисунок 177).

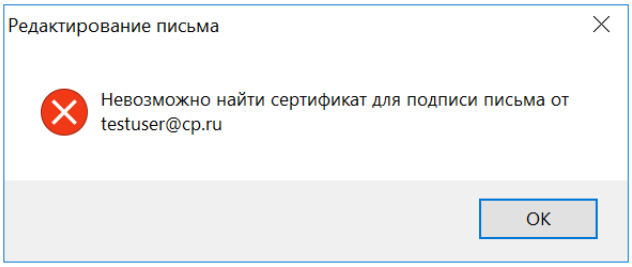


Рисунок 177. Ошибка при подписи письма

7 Использование КриптоПро CSP при работе с почтовым клиентом Microsoft Outlook 2016

СКЗИ КриптоПро CSP позволяет использовать инфраструктуру открытых ключей и стандартные продукты Microsoft (включая приложения электронной почты Microsoft Outlook, Microsoft Outlook Express, Windows Mail и Windows Live Mail) со стойкими российскими криптографическими алгоритмами и ключами 256 бит.

В разделе приведена инструкция по интеграции и настройке работы СКЗИ КриптоПро CSP с почтовым клиентом Microsoft Outlook 2016, входящим в состав пакета Microsoft Office 2016. Использование СКЗИ КриптоПро CSP в Microsoft Outlook 2016 во многом совпадает с использованием в Microsoft Outlook более ранних версий.

7.1 Настройка Microsoft Outlook 2016

Откройте Microsoft Outlook 2016, перейдите в меню **Файл** (**File**) и выберите пункт **Параметры** (**Options**) (см. Рисунок 178).

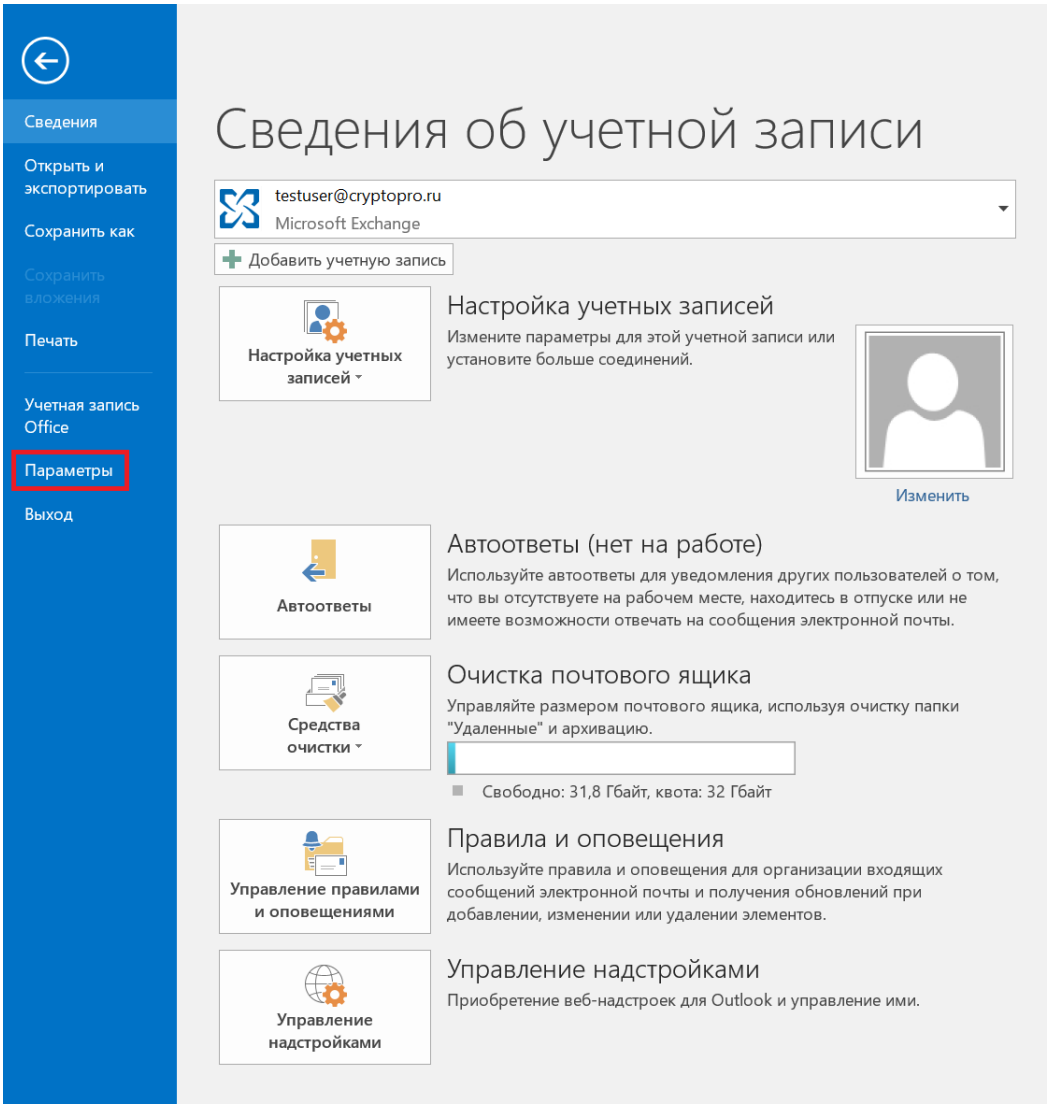


Рисунок 178. Меню **Файл** Microsoft Outlook 2016

В открывшемся окне перейдите на закладку **Центр управления безопасностью** (**Trust Center**) и выберите пункт **Параметры Центра управления безопасностью** (**Trust Center Settings**) (см. Рисунок 179).

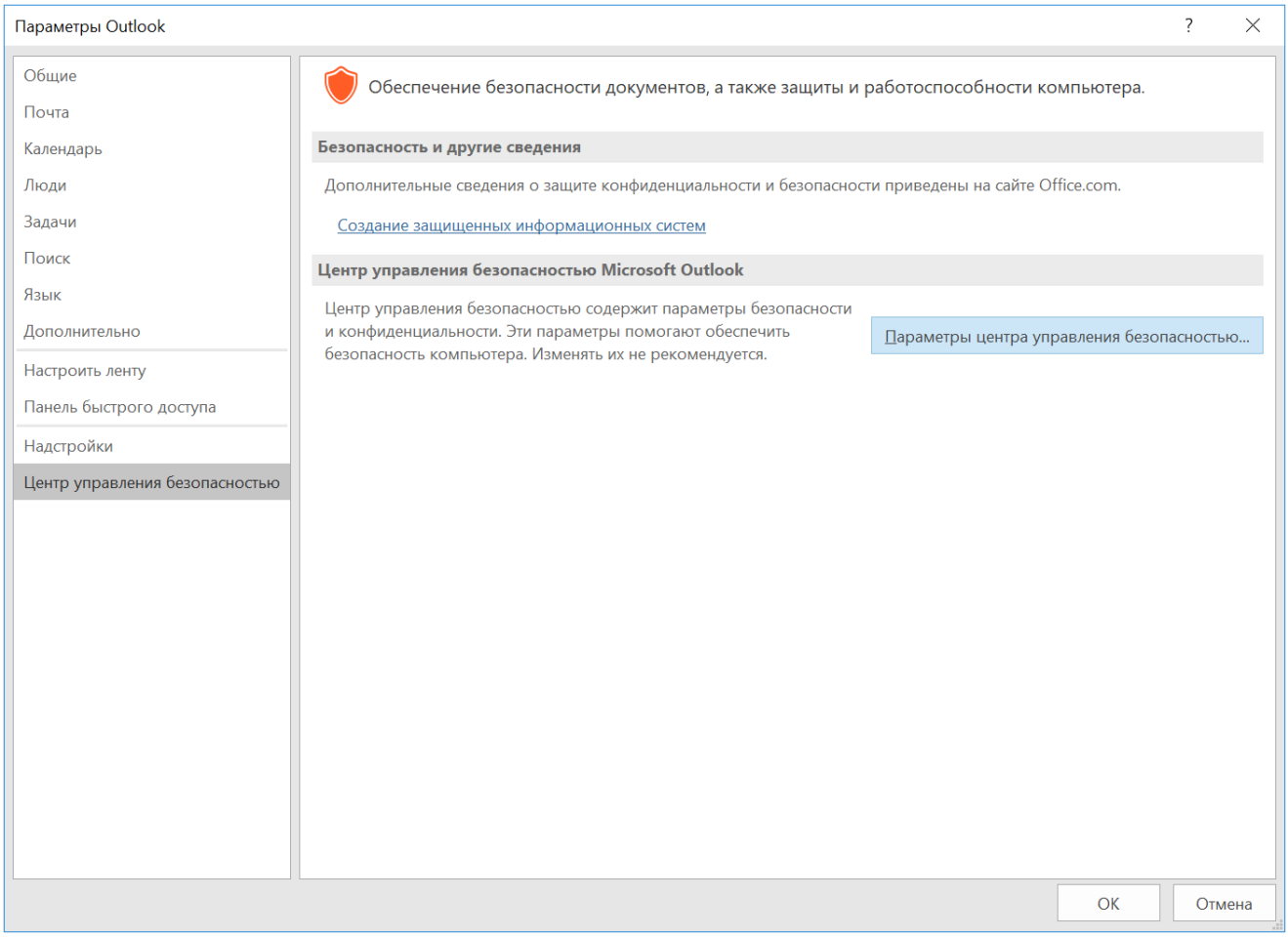


Рисунок 179. Центр управления безопасностью Microsoft Outlook 2016

Далее откройте закладку **Защита электронных писем** (**E-mail Security**) и нажмите кнопку **Параметры** (**Settings**) в секции Шифрованная электронная почта (см. Рисунок 180).

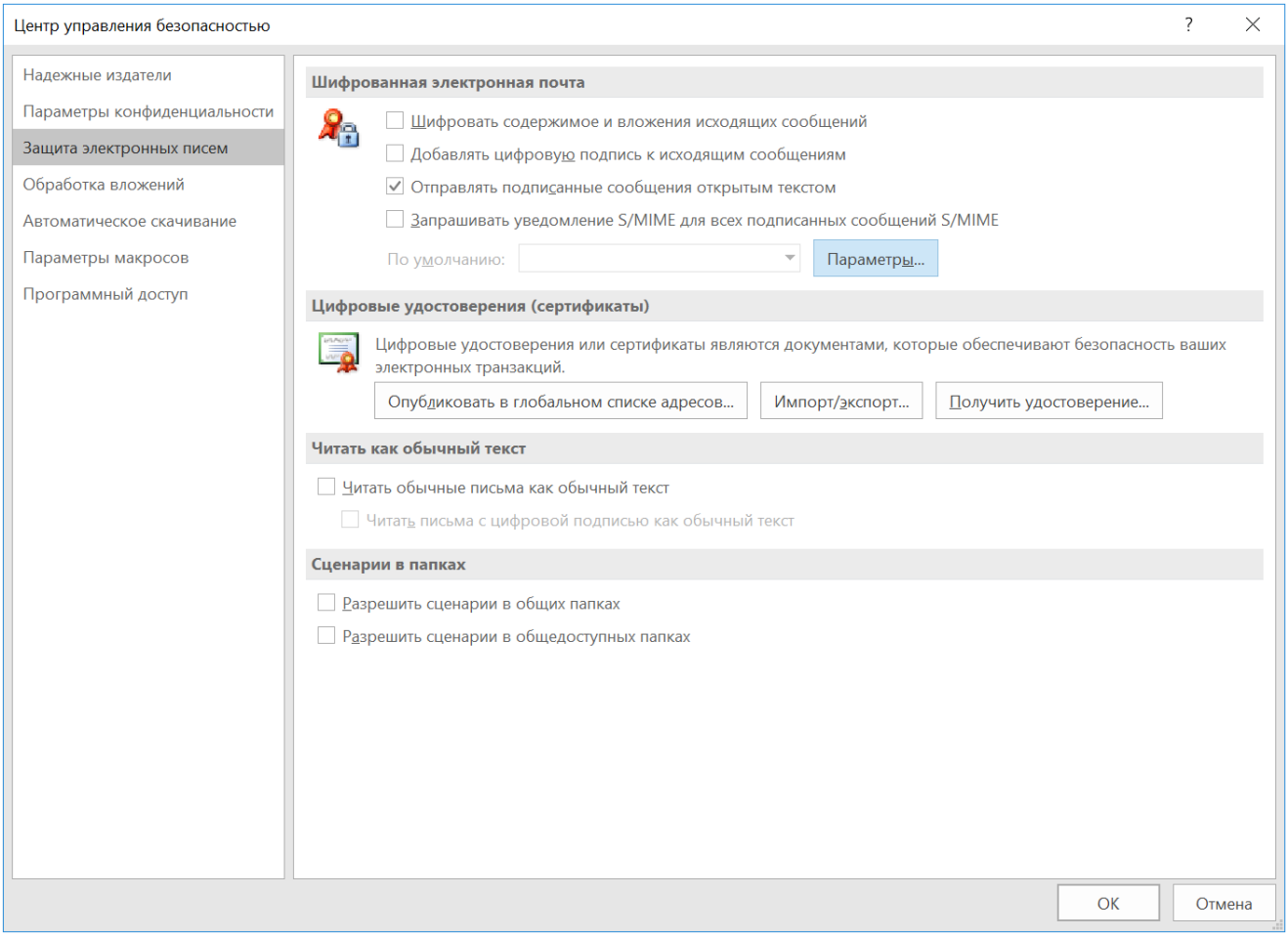


Рисунок 180. Защита электронных писем

В открывшемся окне «Изменение настройки безопасности» (см. Рисунок 181) в секции Сертификаты и алгоритмы выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать** (**Choose**). Отображаемый диалог (см. Рисунок 182) позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной подписи и расшифровки входящих сообщений. Установите флаг **Передавать сертификаты с сообщением** (**Send these certificates with signed messages**). После выбора сертификата укажите **Имя конфигурации** (**Security Settings Name**) и нажмите кнопку **OK**.

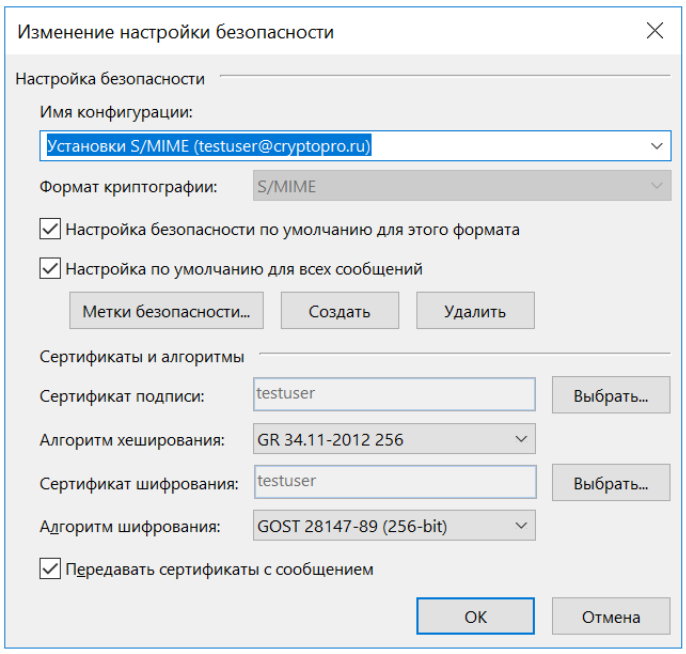


Рисунок 181. Изменение настройки безопасности Microsoft Outlook 2016

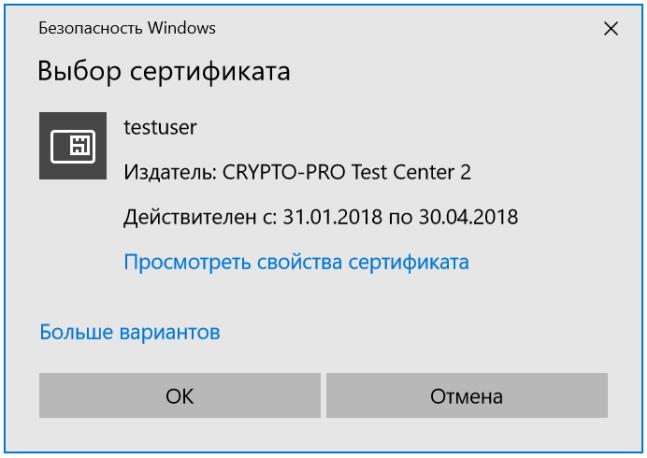


Рисунок 182. Выбор сертификата

На закладке **Защита электронных писем** (**E-mail Security**) можно включить режимы **Шифровать содержимое и вложения исходящих сообщений** (**Encrypt contents and attachments for outgoing messages**) и **Добавлять цифровую подпись к исходящим сообщениям** (**Add digital signature to outgoing messages**) для того, чтобы шифрование и добавление электронной подписи выполнялись автоматически для каждого сообщения. Если эти режимы не включены, опции шифрования и подписи нужно будет включать для каждого отправляемого сообщения.

В этом же диалоге дополнительно можно установить опцию **Отправлять подписанные сообщения открытым текстом** (**Send clear text signed message when sending signed messages**). При включенном режиме подпись формируется в виде одного отдельного вложения для сообщения. Если режим выключен — текст сообщения и все вложения объединяются в единое целое и кодируются в соответствии с правилами кодирования BASE64, после чего результат кодирования подписывается.

7.2 Отправка подписанных сообщений

Для создания и отправки подписанного сообщения нажмите кнопку **Создать сообщение** (**New E-mail**).

Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать

некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** (**Attach File**). Для того, чтобы подписать сообщение, нажмите на кнопку **Подписать** (**Sign**) в закладке **Параметры** (**Options**) (см. Рисунок 183).

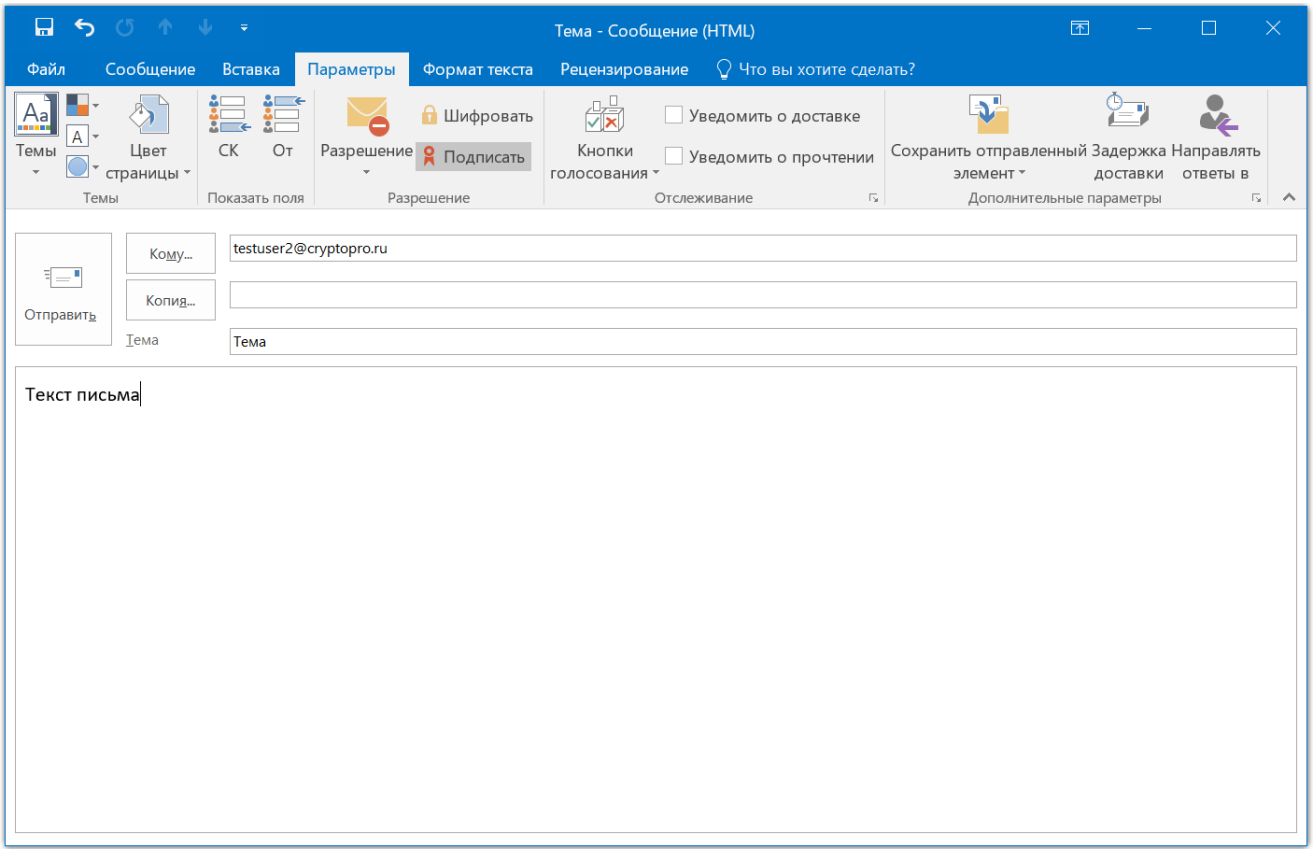


Рисунок 183. Создание подписанного сообщения в Microsoft Outlook 2016

Для отправки сообщения нажмите кнопку **Отправить** (**Send**).

Если сертификат, с помощью которого подписано сообщение, был отозван или электронный адрес, указанный в сертификате, не совпадает с электронным адресом данной учетной записи, то появится предупреждение (см. Рисунок 184), а само сообщение не будет отправлено.

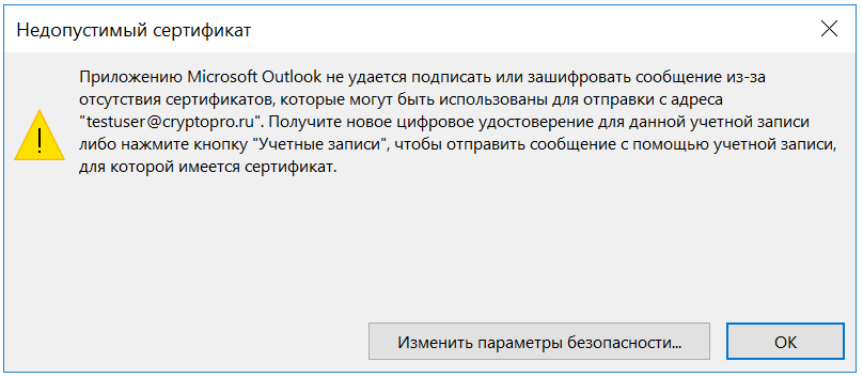


Рисунок 184. Ошибка использования сертификата отправителя в Microsoft Outlook 2016

7.3 Получение сертификата открытого ключа пользователя для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимы сертификаты получателей писем.

Если отправитель и все получатели письма являются пользователями одного домена, то предусмотрена возможность использования глобальной адресной книги. В этом случае необходимо, чтобы сертификаты защиты электронной почты пользователей домена были установлены в AD.

Если для выдачи сертификатов используется ПАК КриптоПро УЦ — можно настроить экспорт издаваемых на УЦ сертификатов в AD, процесс настройки подробно описан в инструкции ЖТЯИ.00067-02 90 05. КриптоПро УЦ. Центр Регистрации. Руководство по эксплуатации, раздел Настройка модуля экспорта сертификатов в Active Directory.

Если УЦ не настроен на публикацию сертификатов в AD, пользователь домена может сам опубликовать свой сертификат, чтобы он был доступен другим пользователям домена для шифрования почты.

Для импорта сертификата в глобальную книгу адресов выполните следующие действия:

1) Откройте закладку **Защита электронных писем** (**E-mail Security**) **Центра управления безопасностью** (**Trust Center**) (подробнее см. разд. 7.1).

2) В разделе Цифровые удостоверения(сертификаты) выберите пункт **Опубликовать в глобальном списке адресов** (**Publish to GAL**) (см. Рисунок 185). Сертификат текущего пользователя, выбранный по умолчанию, будет импортирован в глобальную адресную книгу.

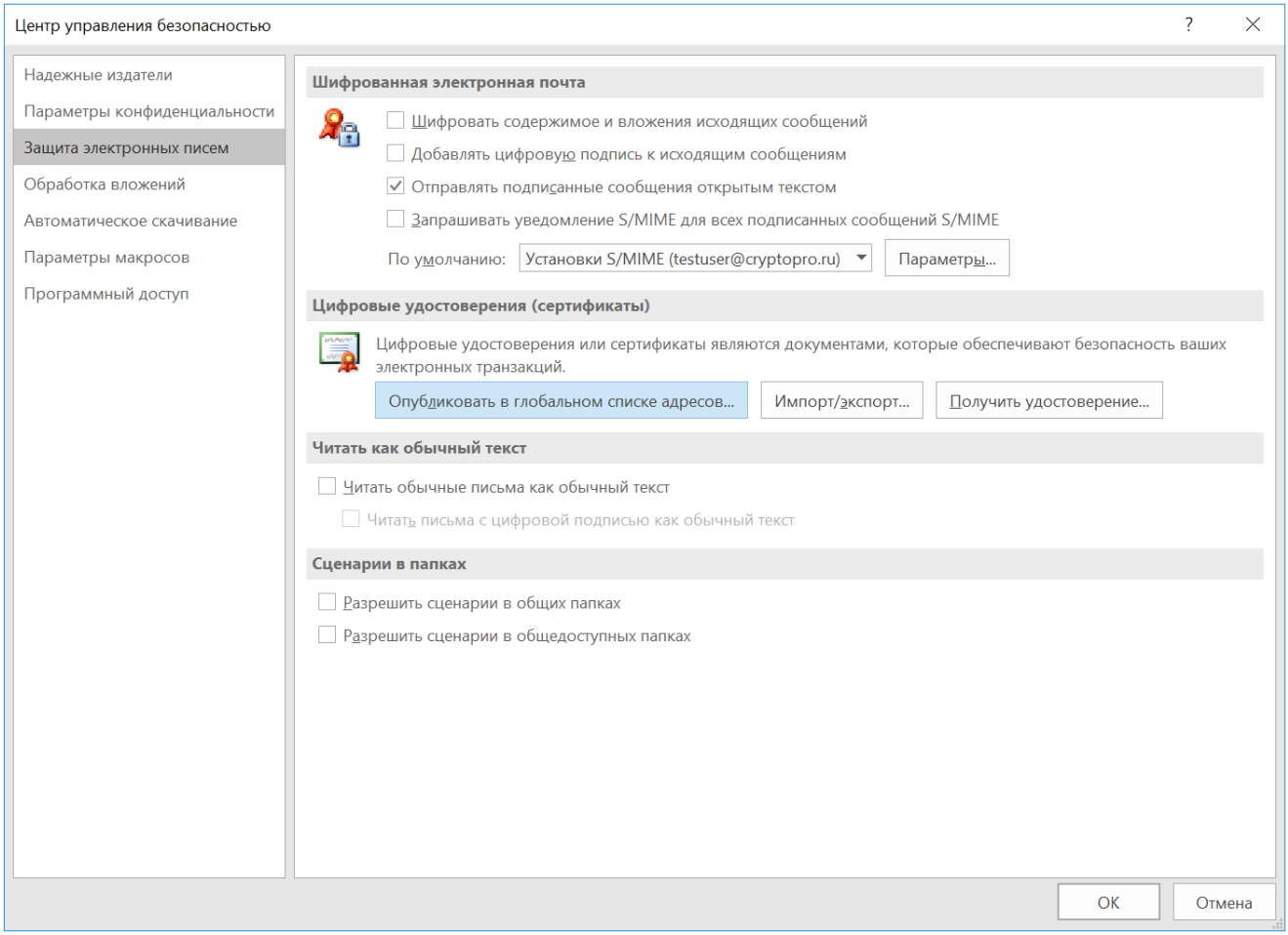


Рисунок 185. Импорт сертификата в глобальную книгу адресов

Из-за особенностей работы программы Outlook обращение в AD за сертификатом получателя письма делается не всегда, вместо этого может использоваться локальная копия адресной книги.

Для актуализации информации о сертификате получателя в локальной копии адресной книги выполните следующие действия:

1) В главном меню Microsoft Outlook 2016 выберите пункт Отправка и получение — Группы отправки и получения. В открывшемся меню выберите Скачать адресную книгу (Рисунок 186).

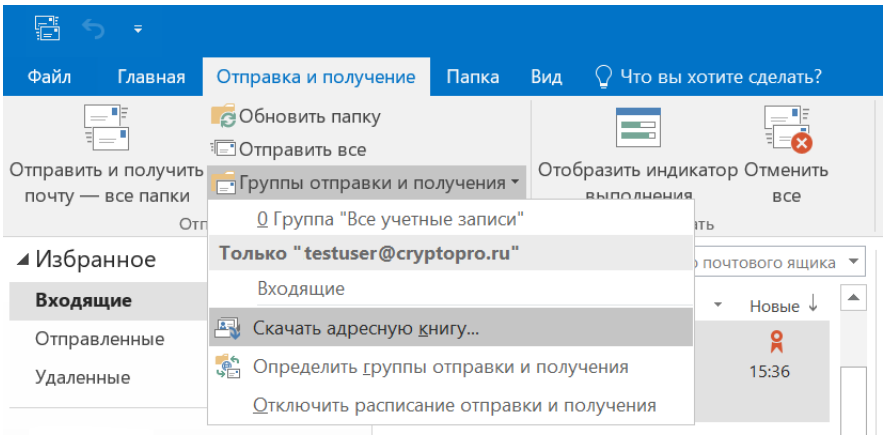


Рисунок 186. Актуализация локальной адресной книги

2) В открывшемся окне (Рисунок 187) выберите адресную книгу и нажмите кнопку **OK**. Информация в адресной книге будет обновлена.

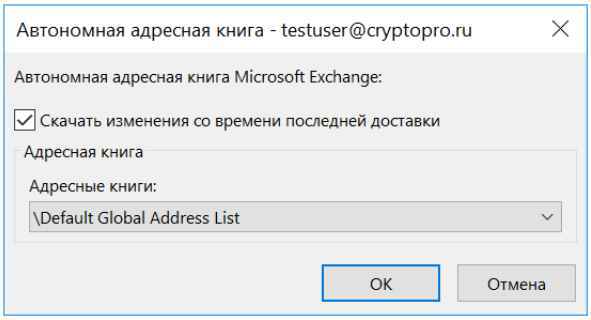


Рисунок 187. Загрузка глобальной книги адресов

Если отправитель и получатели писем не являются пользователями домена или являются пользователями разных доменов или в домене не используется публикация сертификатов для защиты электронной почты, то в качестве источника информации о сертификатах получателей можно использовать список контактов вместо глобальной адресной книги.

Для этого обычно достаточно, чтобы перед тем, как абонент А будет отправлять зашифрованное сообщение в адрес абонента Б, абонент Б прислал абоненту А подписанное сообщение (сообщение посылается вместе с сертификатом абонента Б). Затем нужно добавить отправителя подписанного письма в контакты Outlook. Для этого нажмите правой кнопкой по имени отправителя и выберите пункт **Добавить в контакты Outlook** (см. Рисунок 188).

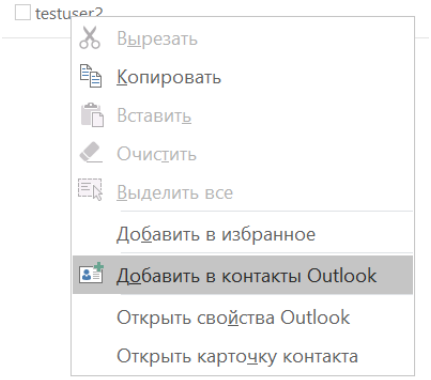


Рисунок 188. Добавление контакта в Microsoft Outlook 2016

Для контроля правильности добавления сертификата выполните следующие действия:

1) Откройте локальную адресную книгу, нажав на кнопку **Адресная книга** секции Найти верхней панели(см. Рисунок 189).

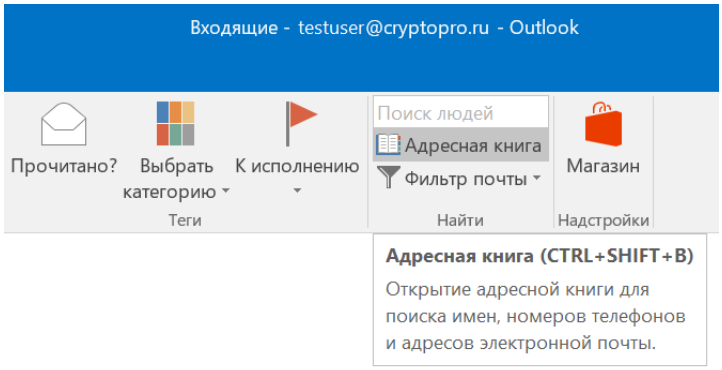


Рисунок 189. Доступ к адресной книге Microsoft Outlook 2016

2) В открывшемся окне (см. Рисунок 190) установите фильтр Контакты текущего пользователя и откройте нужный контакт двойным щелчком мыши.

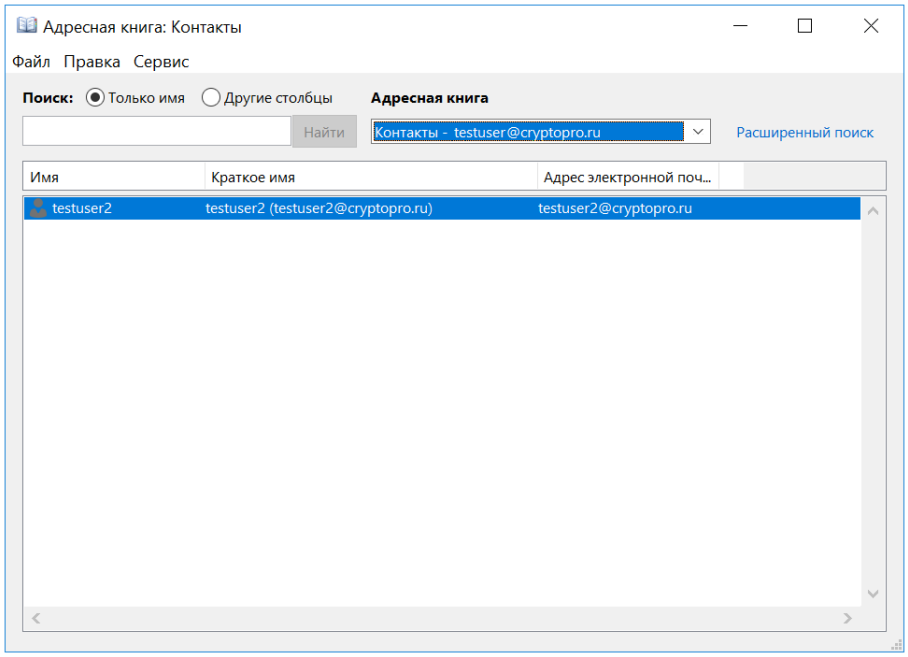


Рисунок 190. Локальная адресная книга Microsoft Outlook 2016

3) В карточке контакта нажмите кнопку **Сертификаты** секции Показ верхней панели (см. Рисунок 191).

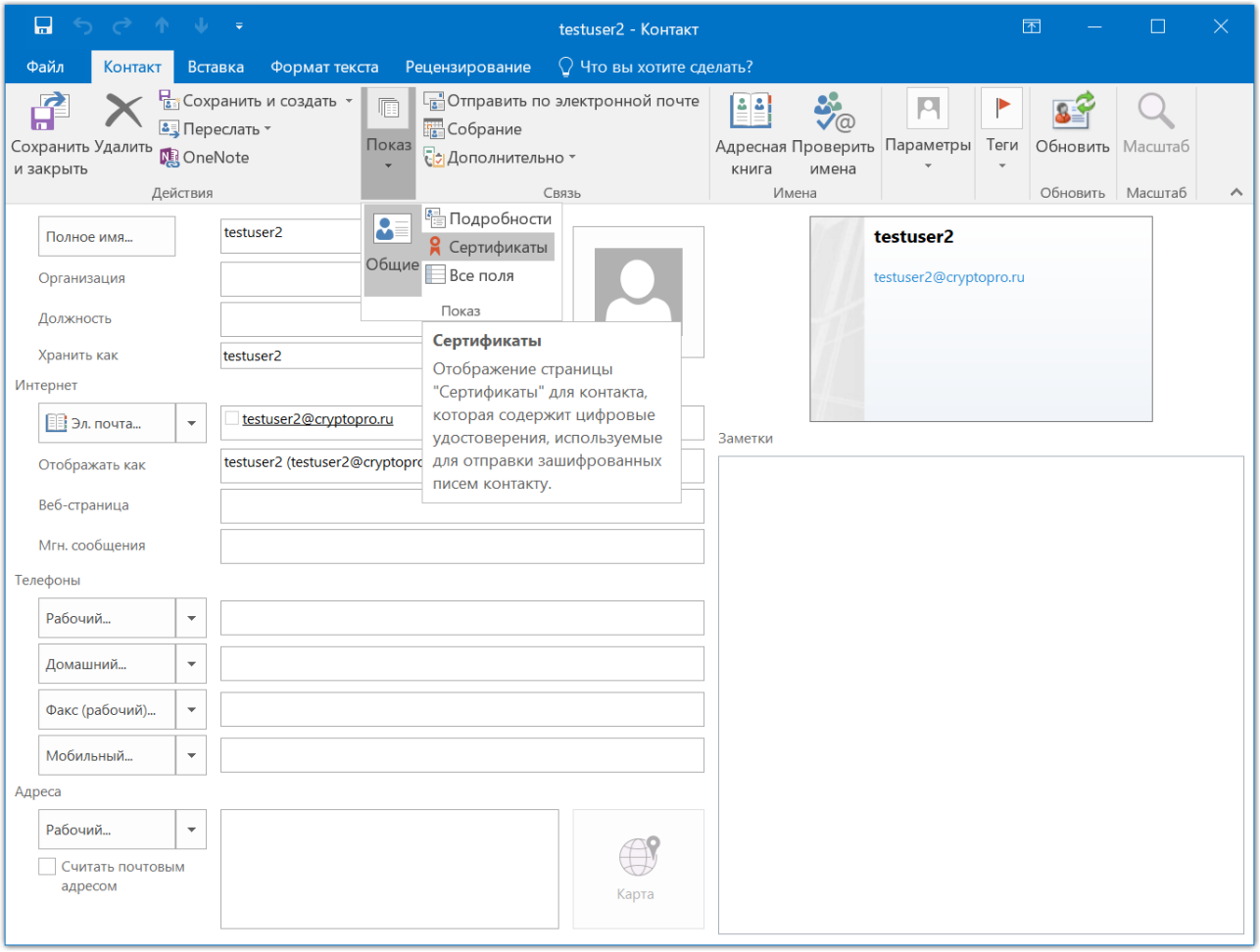


Рисунок 191. Карточка контакта в Microsoft Outlook 2016

4) Убедиться в наличии в открывшемся окне сертификата пользователя (см. Рисунок 192).

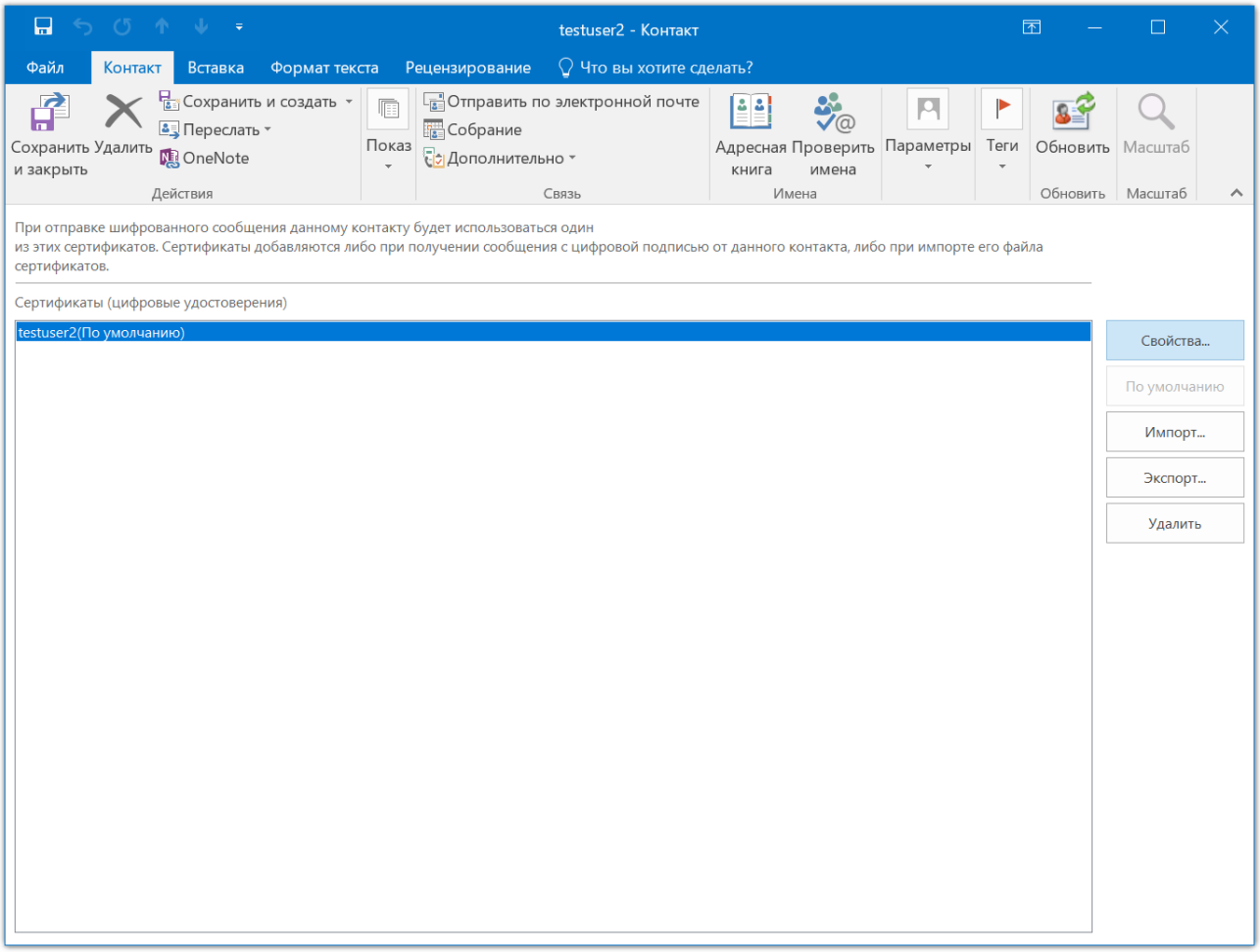


Рисунок 192. Список сертификатов контакта

7.4 Отправка зашифрованных сообщений

Для создания и отправки зашифрованного сообщения нажмите кнопку **Создать сообщение** (**New E-mail**).

Выберите получателя сообщения (поле **To**) и введите тему сообщения (**Subject**). Если письмо будет содержать некоторые файлы, добавьте их в письмо, используя кнопку **Вложить файл** (**Attach File**). Для того, чтобы зашифровать сообщение, нажмите на кнопку **Шифровать** (**Encrypt**) в закладке **Параметры** (**Options**) (см. Рисунок 193).

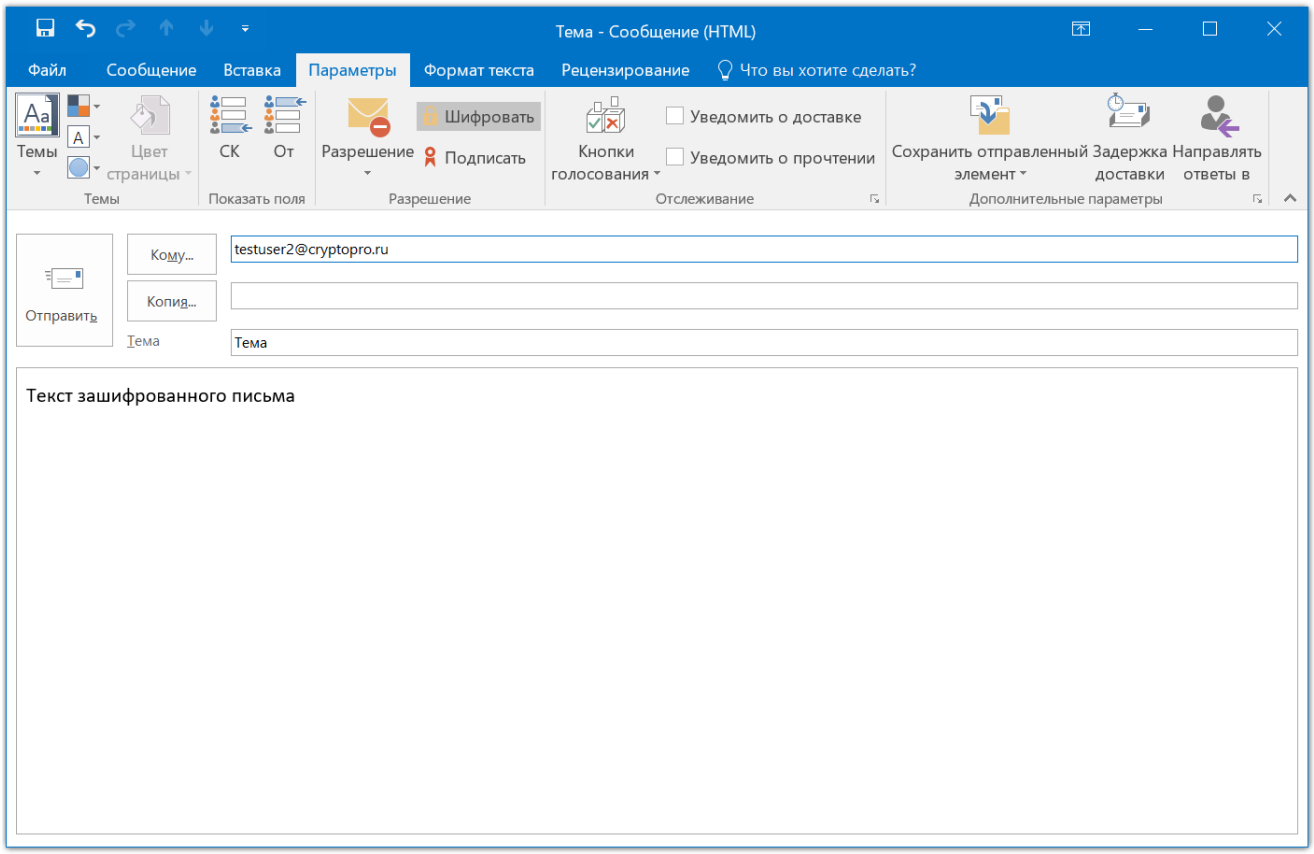


Рисунок 193. Создание зашифрованного сообщения в Microsoft Outlook 2016

Для отправки сообщения нажмите кнопку **Отправить** (**Send**).

Если при попытке зашифровать письмо не удалось найти сертификат получателя или сертификат недействителен (например, истек или отозван), появится следующее предупреждение (см. Рисунок 194).

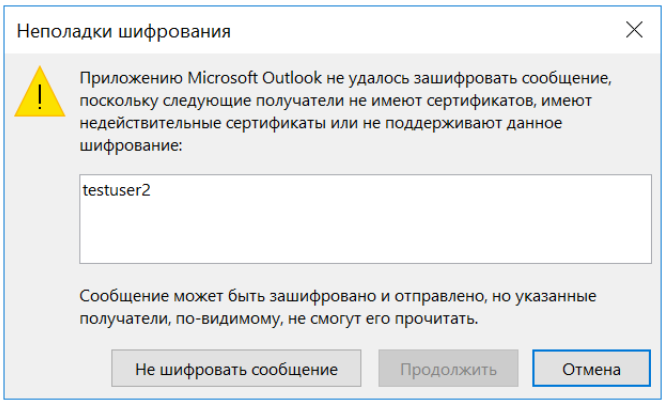


Рисунок 194. Ошибка при шифровании сообщения

7.5 Просмотр зашифрованных сообщений

Просмотр зашифрованных сообщений доступен только пользователям, у которых установлен сертификат, который использовался отправителем при шифровании сообщения.

Для просмотра сведений о сертификате пользователя откройте полученное от него зашифрованное письмо и

нажмите кнопку  — признак зашифрованного сообщения.

Откроется окно свойств безопасности зашифрованного сообщения (см. Рисунок 195).

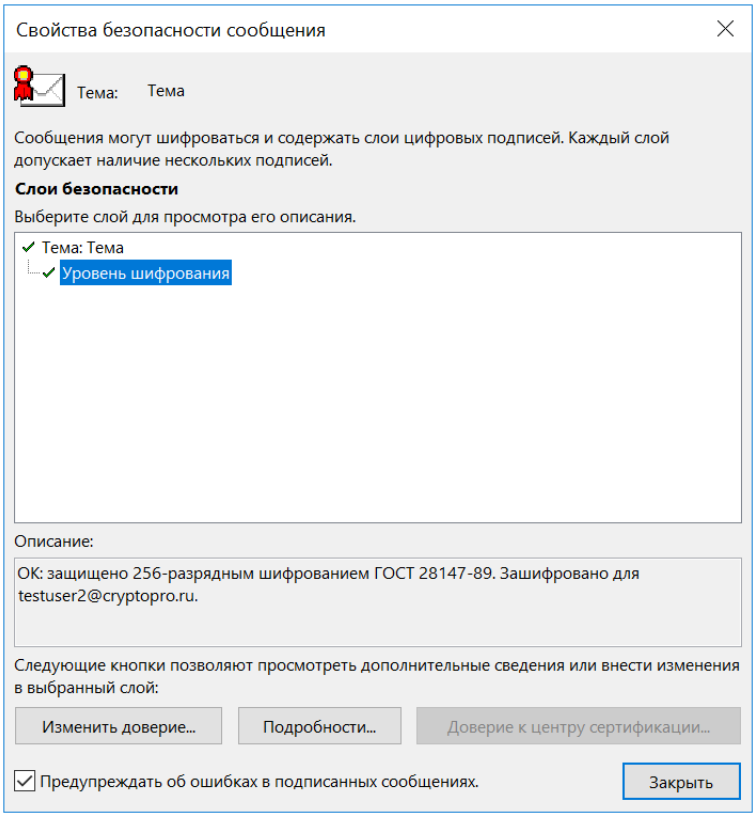


Рисунок 195. Сведения о шифровании сообщения

Если у получателя зашифрованного письма отсутствует сертификат, который использовался при шифровании данного сообщения, просмотр содержимого письма недоступен и в окне Microsoft Outlook 2016 отображается следующее сообщение (см. Рисунок 196).

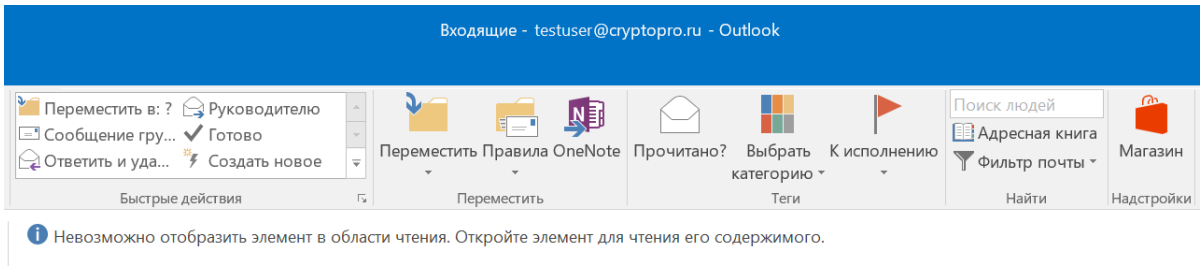


Рисунок 196. Просмотр зашифрованного сообщения при отсутствии сертификата

Если получатель попытается открыть сообщение, откроется окно с ошибкой (см. Рисунок 197).

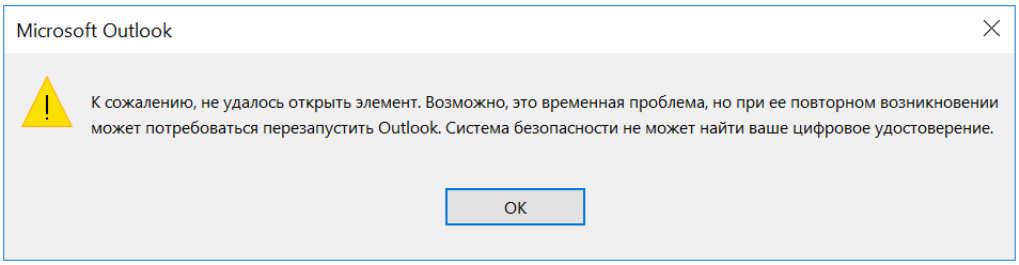


Рисунок 197. Ошибка просмотра зашифрованного сообщения

7.6 Проверка сертификата отправителя подписанного сообщения

Для проверки сертификата пользователя откройте полученное от него подписанное письмо и нажмите кнопку — признак подписанного сообщения.

Откроется окно проверки цифровой подписи (см. Рисунок 198).

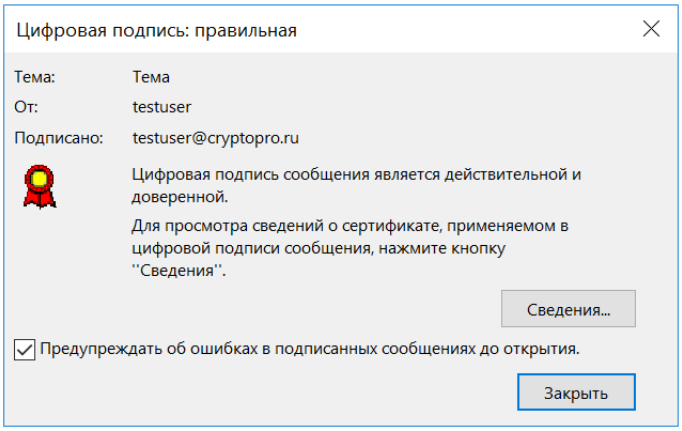


Рисунок 198. Проверка цифровой подписи

Для просмотра сведений о сертификате нажмите кнопку **Сведения** (**Details**). Если вы видите следующее окно (см. Рисунок 199), это означает, что сертификат отправителя письма является действительным.

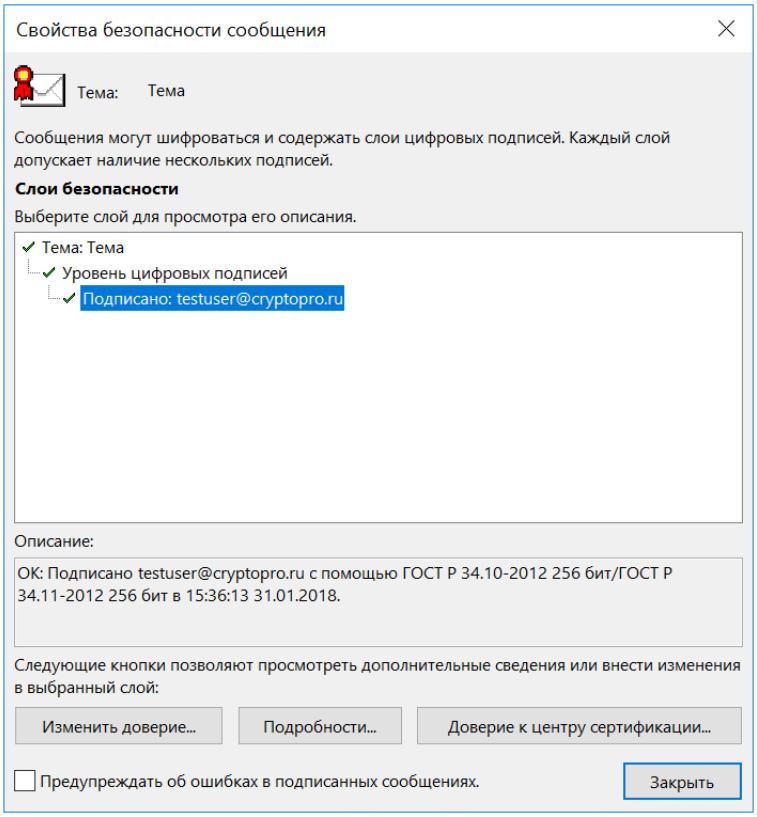


Рисунок 199. Сведения о цифровой подписи

Если сертификат отправителя подписанного письма выдан тем УЦ, к которому нет доверия на компьютере получателя, то при открытии подписанного письма появится следующее предупреждение (см. Рисунок 200).

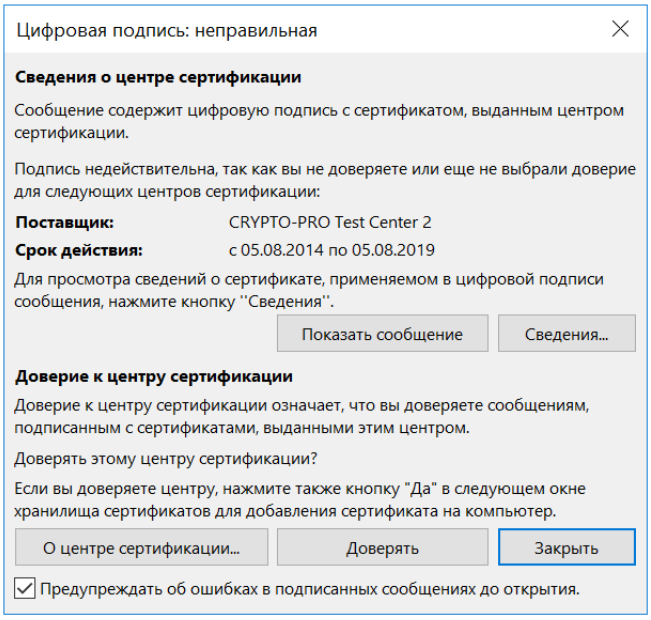


Рисунок 200. Предупреждение о сертификате, выданном УЦ без доверия

Если не удалось проверить действительность сертификата отправителя подписанного письма или если этот сертификат был отозван, то при открытии подписанного письма появится предупреждение (см. Рисунок 201).

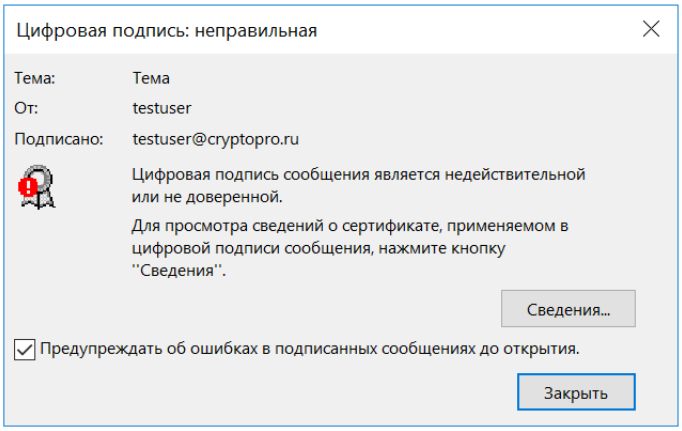


Рисунок 201. Сообщение о недействительной цифровой подписи

Нажмите кнопку **Сведения** (**Details**) для просмотра сведений о сертификате. Если сертификат отправителя был отозван, появится окно с информацией об этом (см. Рисунок 202).

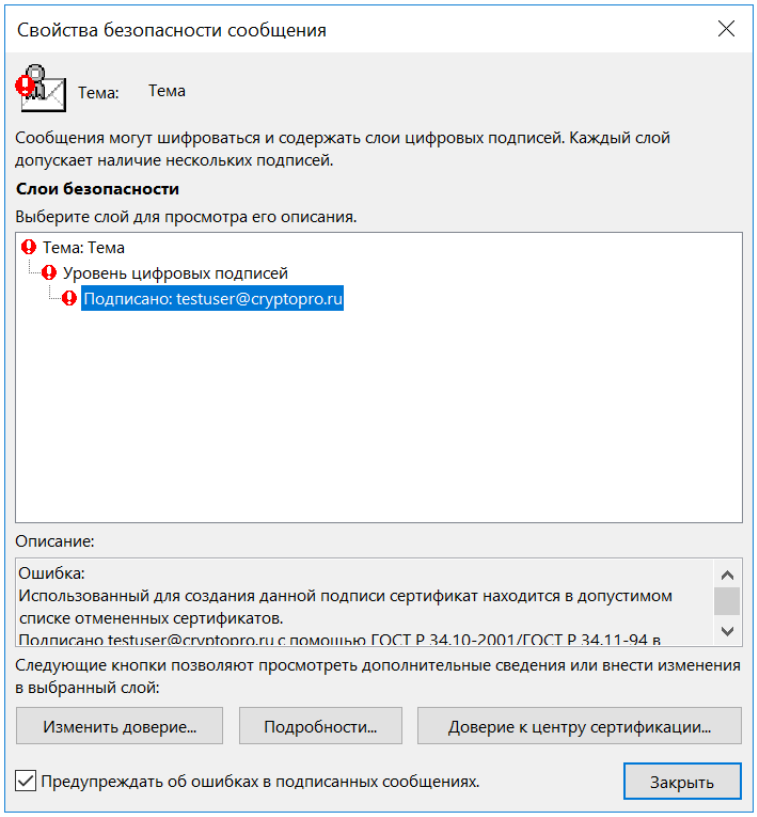


Рисунок 202. Сведения об отозванном сертификате отправителя

Если сертификат отправителя письма не удалось проверить, появится следующее окно с информацией об этом (см. Рисунок 203).

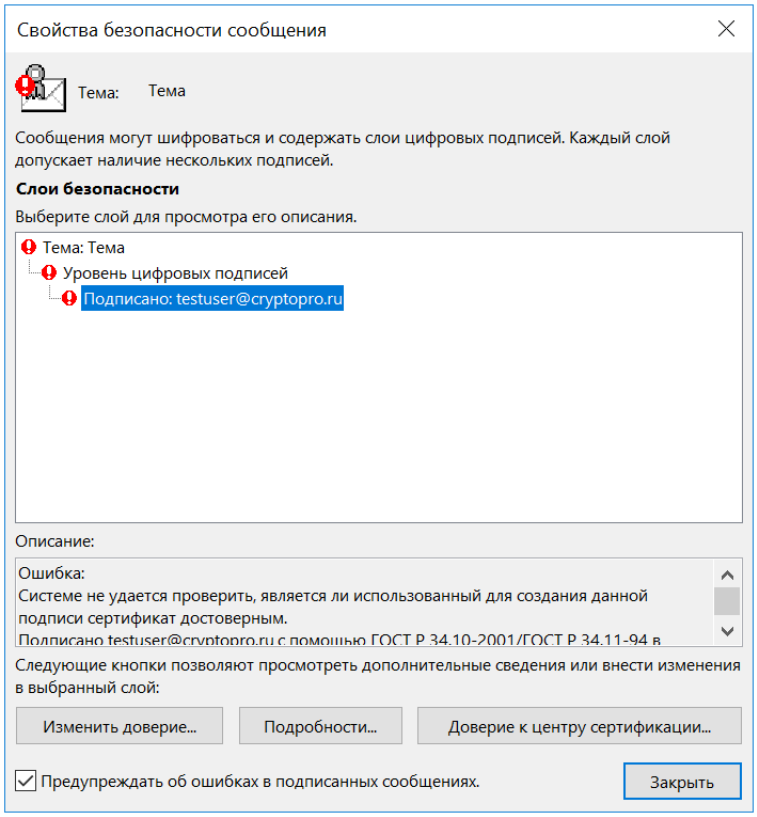


Рисунок 203. Ошибка проверки сертификата

Данная ошибка может появится, если в сертификате отправителя отсутствуют или недоступны или содержат неактуальную информацию точки распространения COC и/или адреса служб OCSP, и при этом COC того УЦ, который выдал сертификат отправителя, не установлен на компьютере получателя, либо срок его действия истек. В таком случае установите актуальный COC в хранилище сертификатов на компьютере получателя для проверки сертификата отправителя.

Если проверка цифровой подписи невозможна или подпись признана недействительной, то предварительный просмотр содержимого письма недоступен, и в окне Microsoft Outlook 2016 отображается следующее сообщение (см. Рисунок 204).

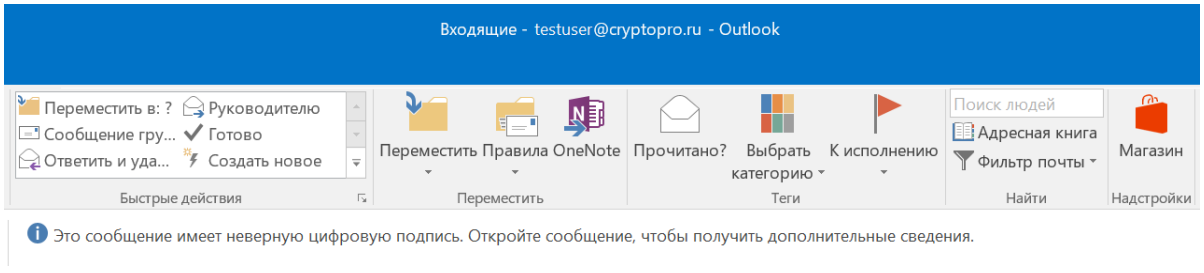


Рисунок 204. Просмотр сообщения с некорректной цифровой подписью