127 018, Москва, Сущевский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP

Версия 4.0 R4 КС2

2-Base

Инструкция по использованию СКЗИ под управлением ОС Windows

ЖТЯИ.00088-03 92 01
Листов 122

2018 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.

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.

Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности (кнопка **Опции**).

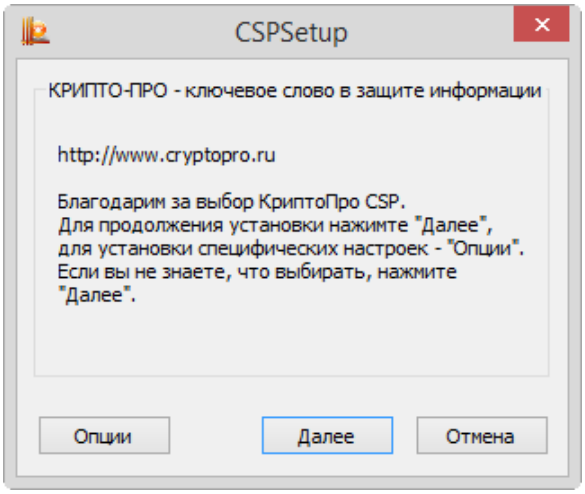


Рисунок 2. Начало установки

В СКЗИ КриптоПро реализованы классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России.

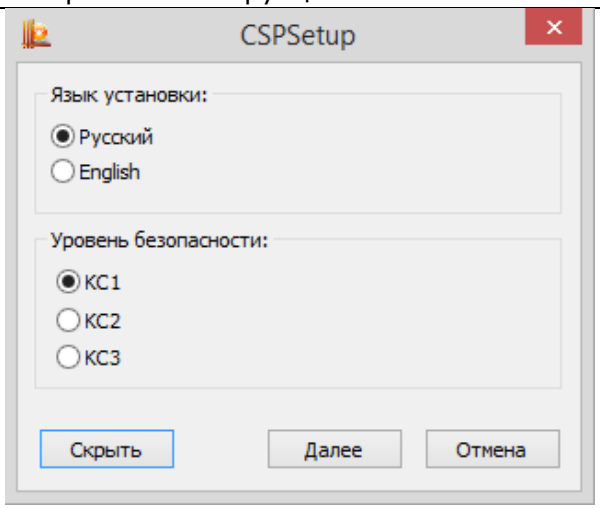


Рисунок 3. Выбор уровня безопасности

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию. После этого можно переходить к работе с мастером установки.

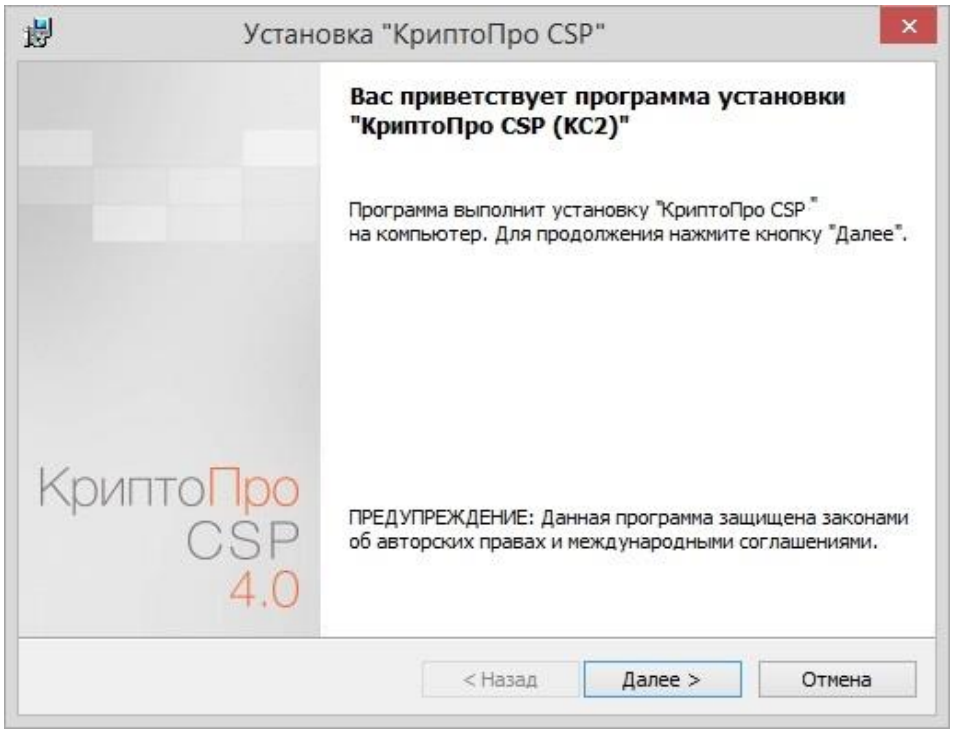


Рисунок 4. Приветственное окно мастера установки

Если на машине была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии:

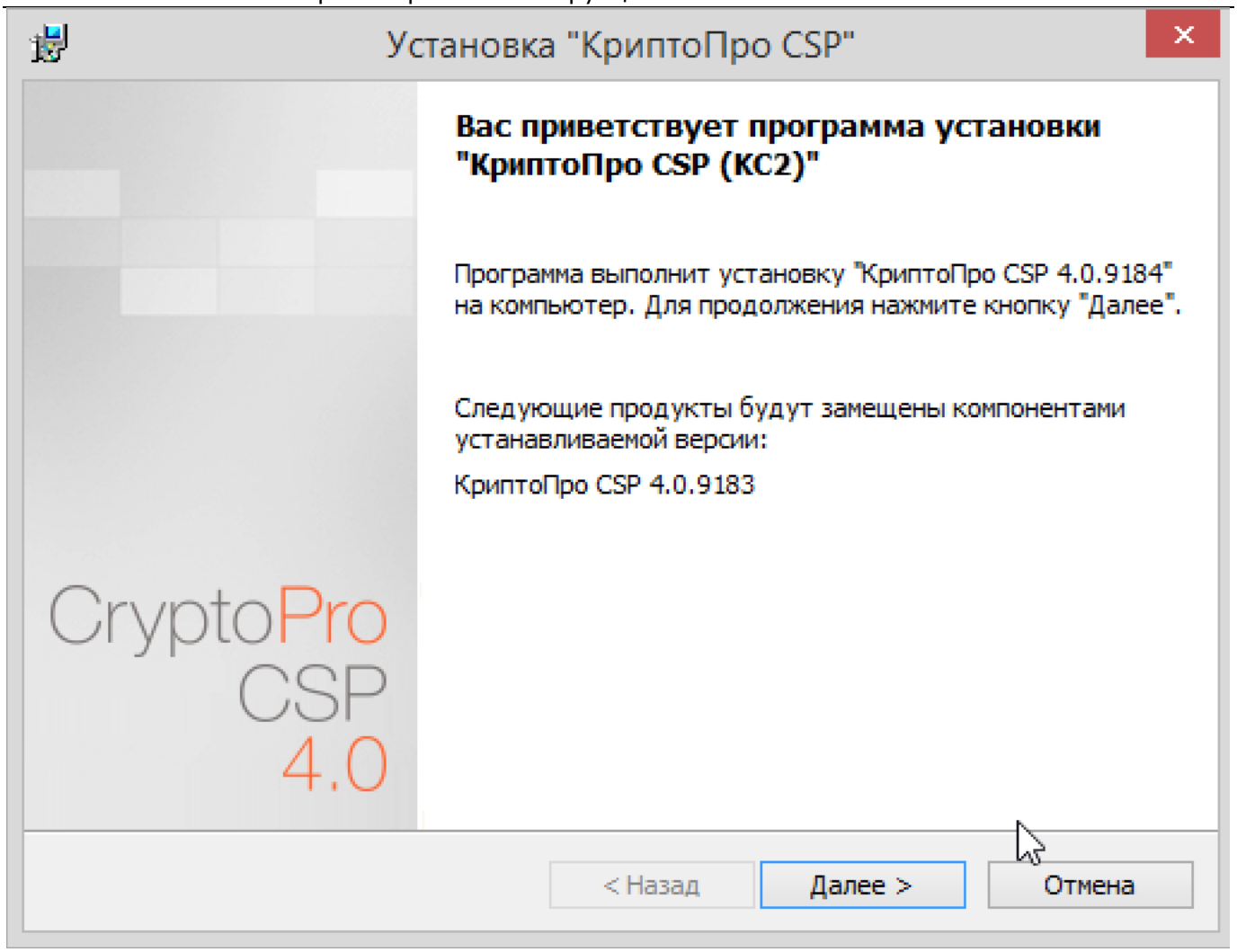


Рисунок 5. Установка с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите **Далее**.

Внимательно прочитайте лицензионное соглашение, которое выводится при первой установке.

Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми мастером.

В процессе установки может быть предложено:

- ввести серийный номер лицензии криптопровайдера;
- зарегистрировать дополнительные считыватели ключевой информации;
- настроить дополнительные датчики случайных чисел;

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

Для корректной работы КриптоПро CSP после завершения установки необходимо перезагрузить компьютер в случае, если пользователю предлагается перезагрузка.

В процессе установки мастером может быть предложен выбор наиболее подходящего вида установки.

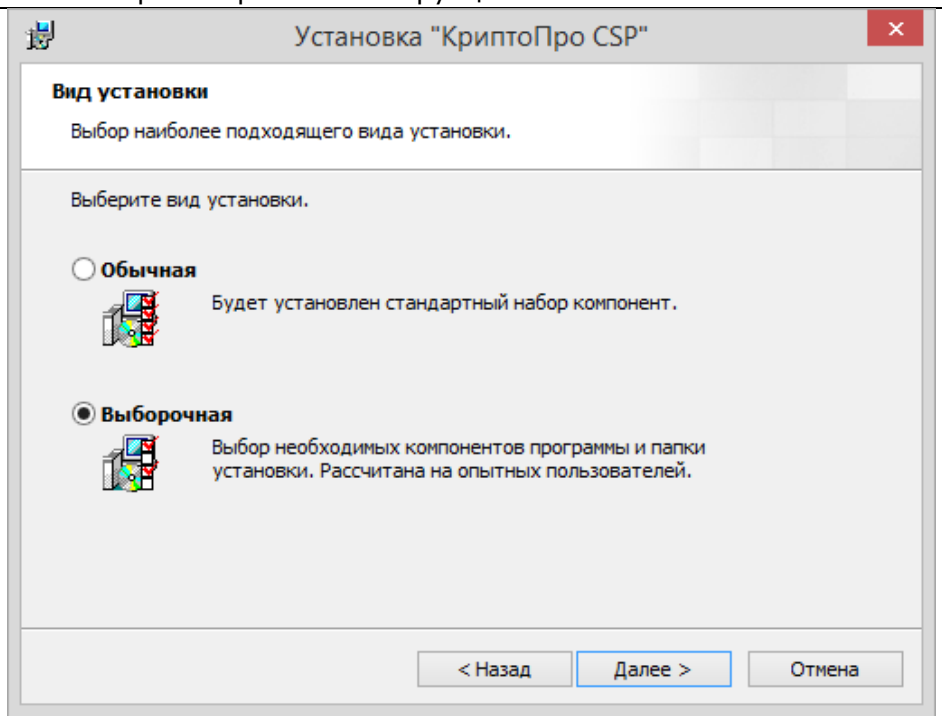


Рисунок 6. Выбор вида установки

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 можно изменить набор компонентов для установки:

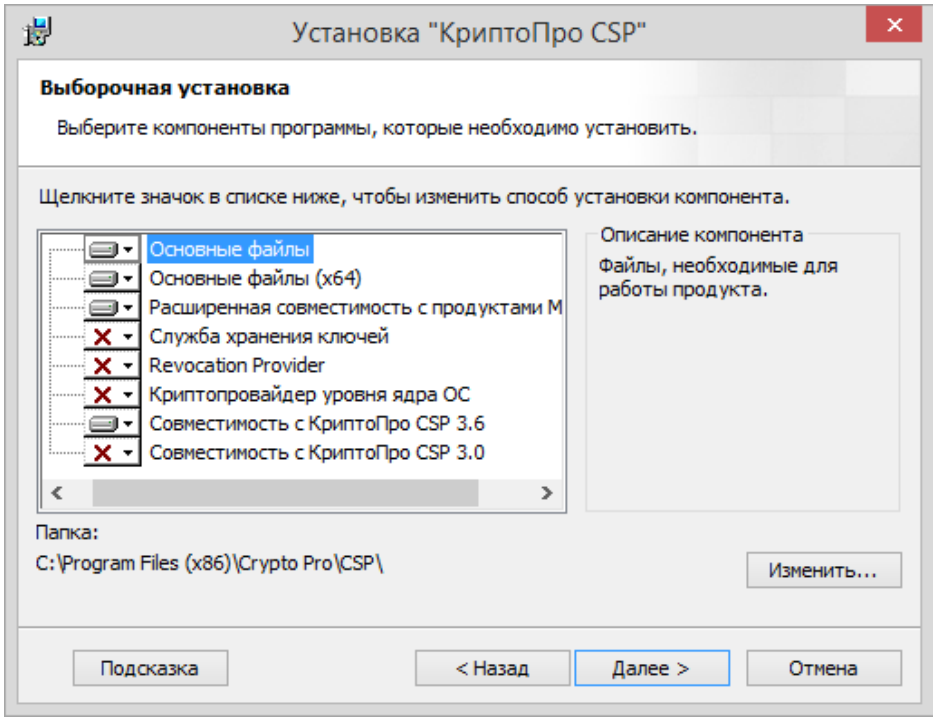


Рисунок 7. Выборочная установка

Расширенная совместимость с продуктами Microsoft – Обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express. Необходима для входа в систему по смарт-картам.

Служба хранения ключей – Обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС. По умолчанию включена для уровня безопасности КС2 и КС3 (подробно описана в разделе Установка параметров безопасности).

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.

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. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.

Совместимость с КриптоПро CSP 3.0 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.0. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.0.

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 **Далее** мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей, а также принять решение о включении функционала накопления информации об использованных съёмных ключевых носителях. Помимо этого, 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 4.0 R4 без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

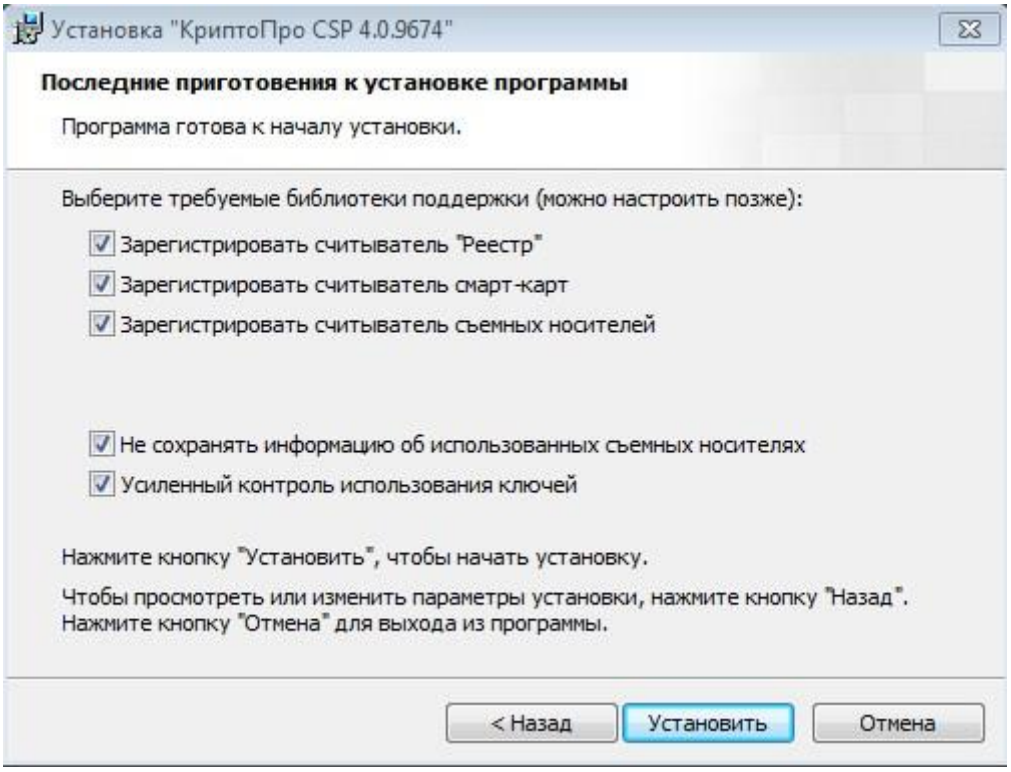


Рисунок 8. Установка усиленного контроля использования ключей

При установке СКЗИ с включением режима усиленного контроля использования ключей будут запрошены данные с датчика случайных чисел. В случае ошибки получения данных будет отображено окно, пример которого приведён на Рисунок 9. В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP 4.0 R4 необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, внешняя гамма или аппаратный ДСЧ), и выполнить команду:

csptest.exe -keyset -verifycontext -hard_rng.

После завершения установки СКЗИ с включённым 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 ca.cer

После этого следует осуществить перезагрузку компьютера.

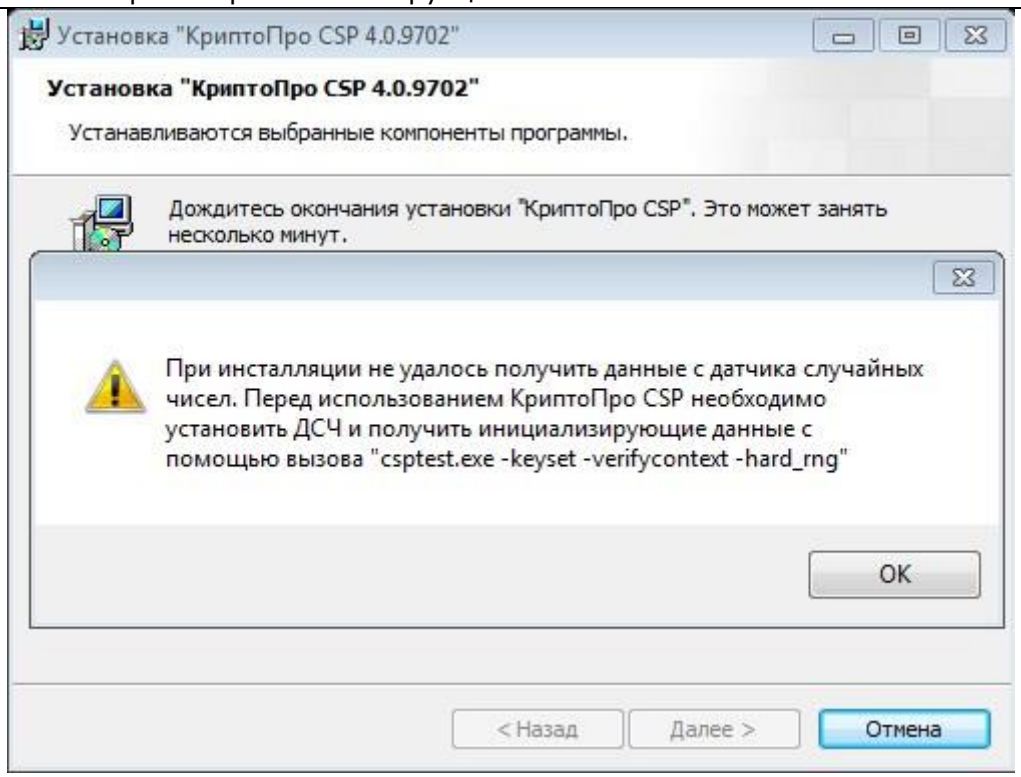


Рисунок 9. Окно ошибки получения данных с датчика случайных чисел при инсталляции СКЗИ.

2. Интерфейс СКЗИ КриптоПро CSP

2.1. Доступ к панели управления СКЗИ

Контрольная Панель управления средства криптографической защиты информации (СКЗИ) КриптоПро CSP доступна как отдельный пункт в группе программ «КРИПТО-ПРО» (меню **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **КриптоПро CSP**).

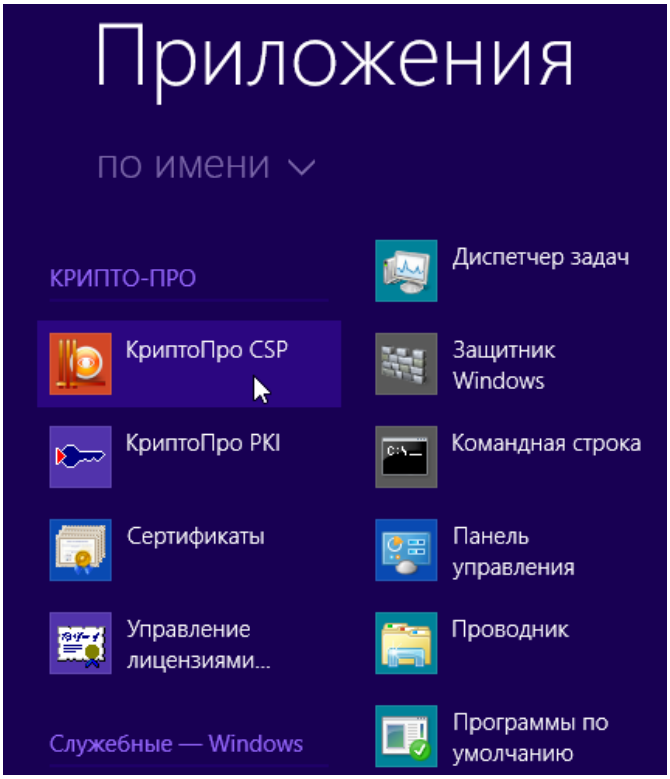


Рисунок 10. Доступ к оснастке

Панель управления СКЗИ КриптоПро CSP осуществляет доступ к настройке функций с помощью вкладок:

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

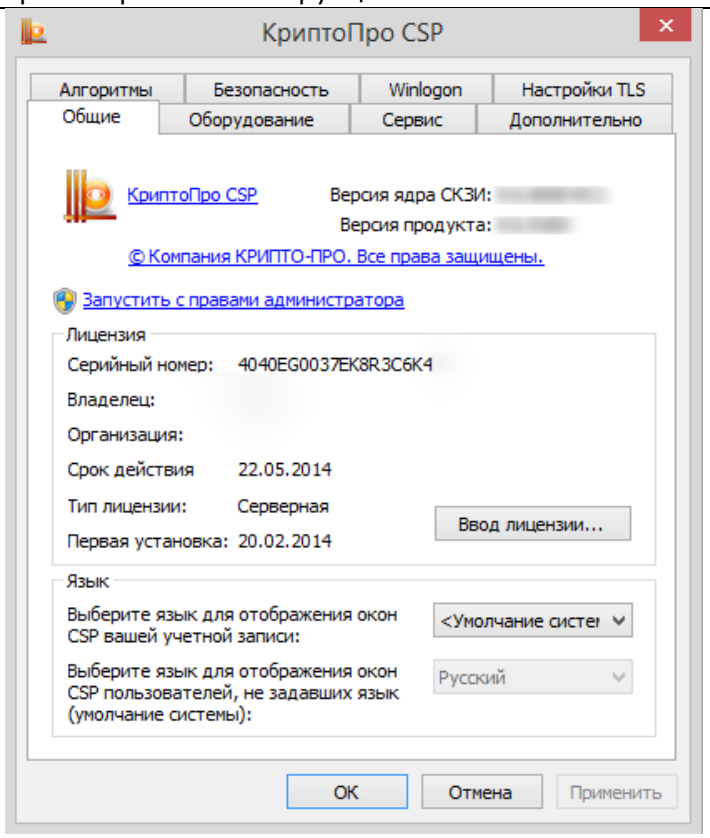


Рисунок 11. Панель управления

2.2. Общие параметры СКЗИ

Вкладка **Общие** (см. Рисунок 11) 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 криптопровайдера «КриптоПро CSP»), изменения языка работы пользователя с данным ПО.

2.3. Ввод серийного номера лицензии криптопровайдера «КриптоПро CSP»

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 13).

Также можно ввести лицензию с помощью утилиты Управление лицензиями КриптоПро PKI. Для этого выполните **Пуск ⇒ Программы ⇒ КриптоПро ⇒ 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 12).

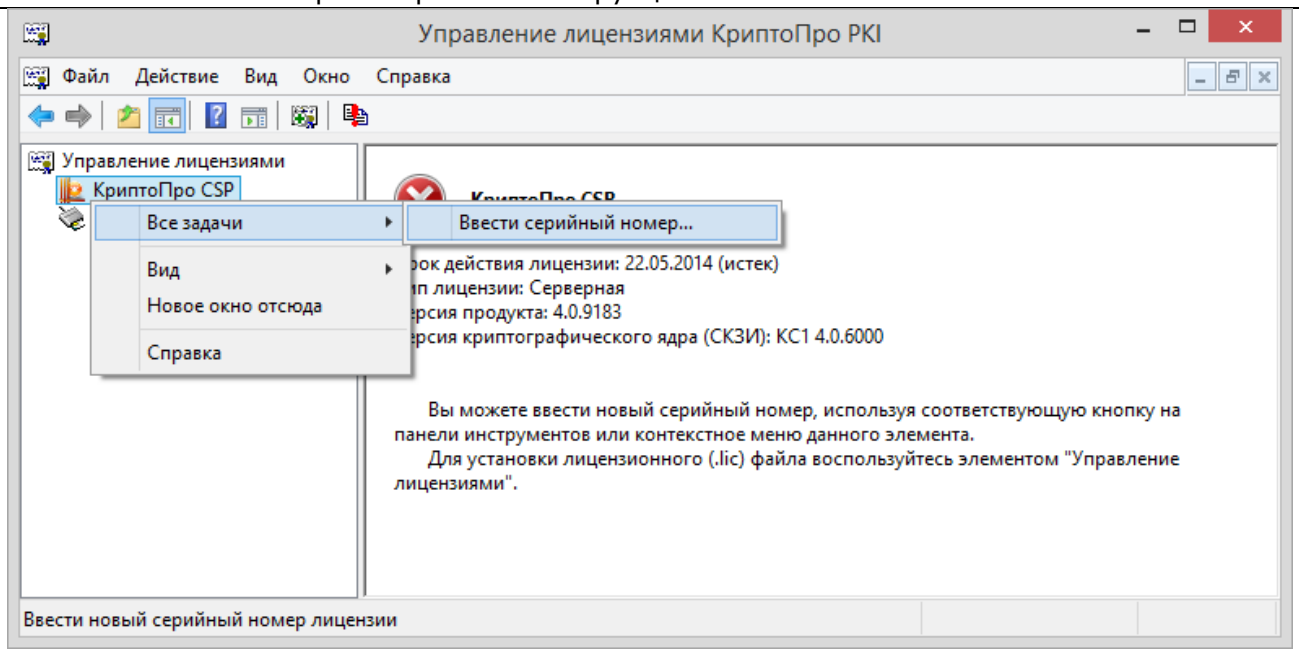


Рисунок 12. Ввод серийного номера

Откроется окно «Сведения о пользователе», в котором необходимо указать сведения о пользователе, организации, а также ввести **серийный номер** с бланка **Лицензии** в соответствующие поля ввода (см. Рисунок 13).

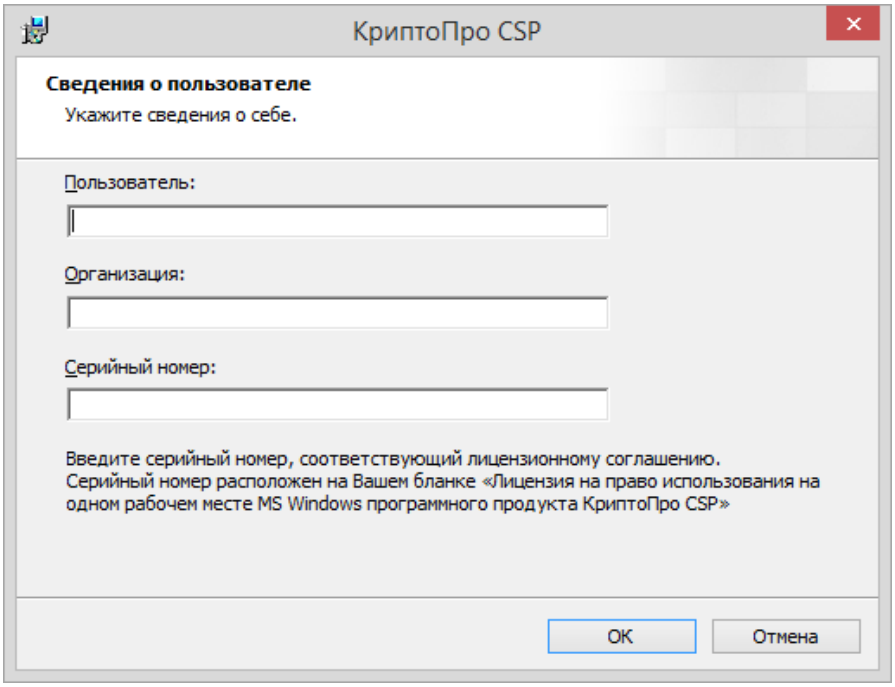


Рисунок 13. Ввод данных лицензии

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

2.4. Настройка оборудования СКЗИ

Вкладка **Оборудование** контрольной панели СКЗИ предназначена для изменения набора устройств хранения и считывания ключевой информации и датчиков случайных чисел (ДЧС).

По умолчанию поддерживаются все считыватели смарт-карт (и соответствующие им типы носителей), все дисководы съемных дисков, в том числе flash-носители.

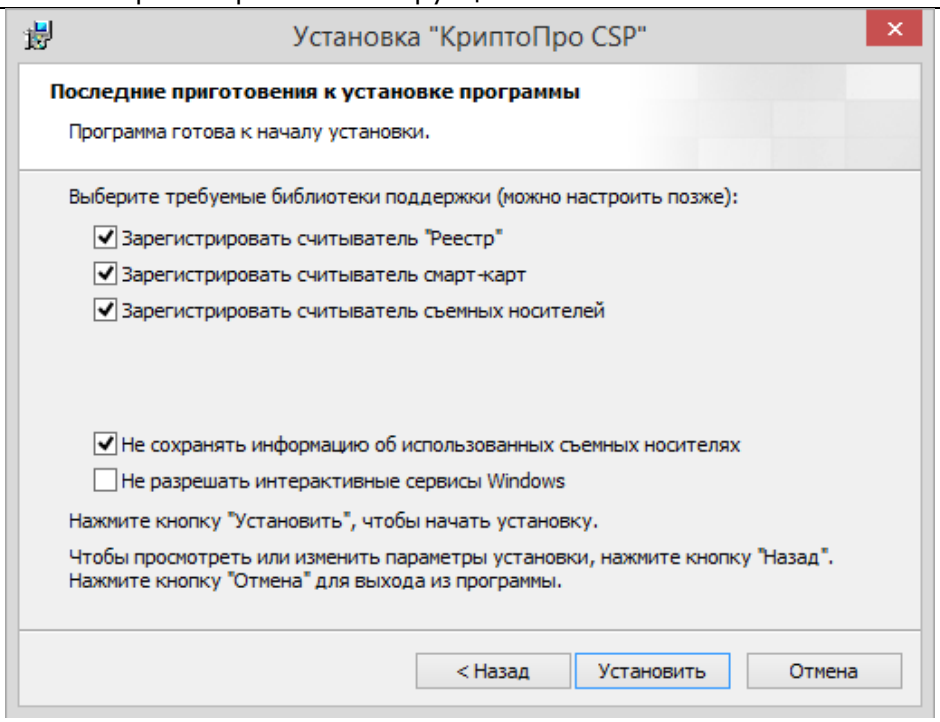


Рисунок 14. Настройка оборудования по уровню защиты КС1

В исполнении по уровню защиты КС1 предустановлен Биологический ДСЧ. В исполнениях по уровням защиты КС2 и КС3 Биологический ДСЧ / аппаратный ДСЧ «Соболь» / АПМДЗ-У М-526Б (КРИПТОН ЗАМОК/У), АПМДЗ-Е М-526Е1 (КРИПТОН ЗАМОК/Е) / АПМДЗ «МАКСИМ-М1» можно добавить в процессе установки криптопровайдера.

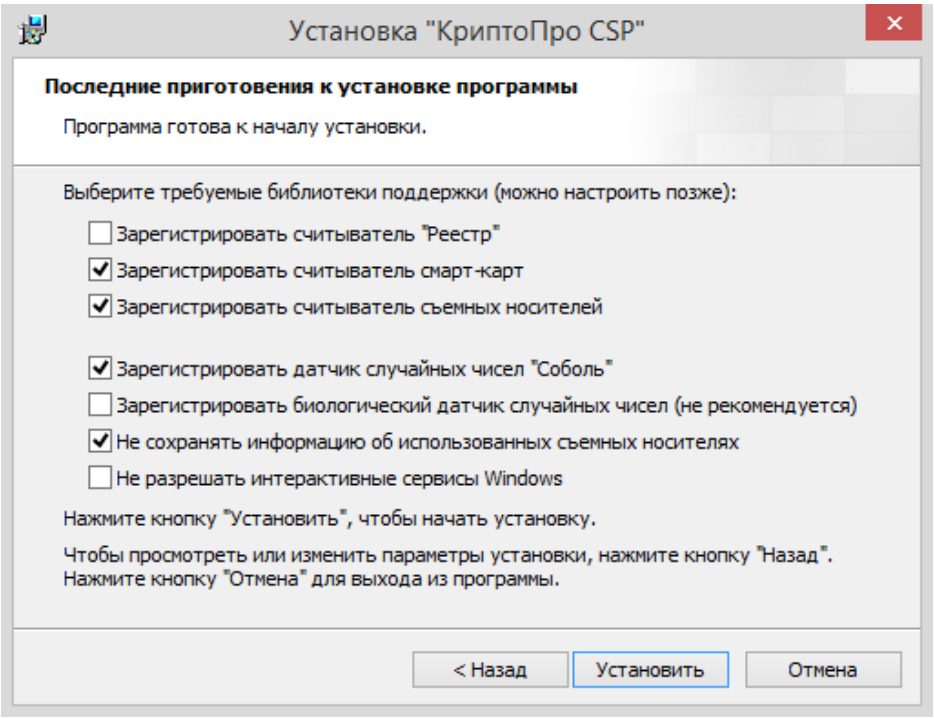


Рисунок 15. Настройка оборудования по уровням защиты КС2 и КС3

2.4.1. Изменение набора устройств считывания ключевой информации

2.4.1.1. Добавление считывателя

Для того, чтобы добавить считыватель, 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели.**

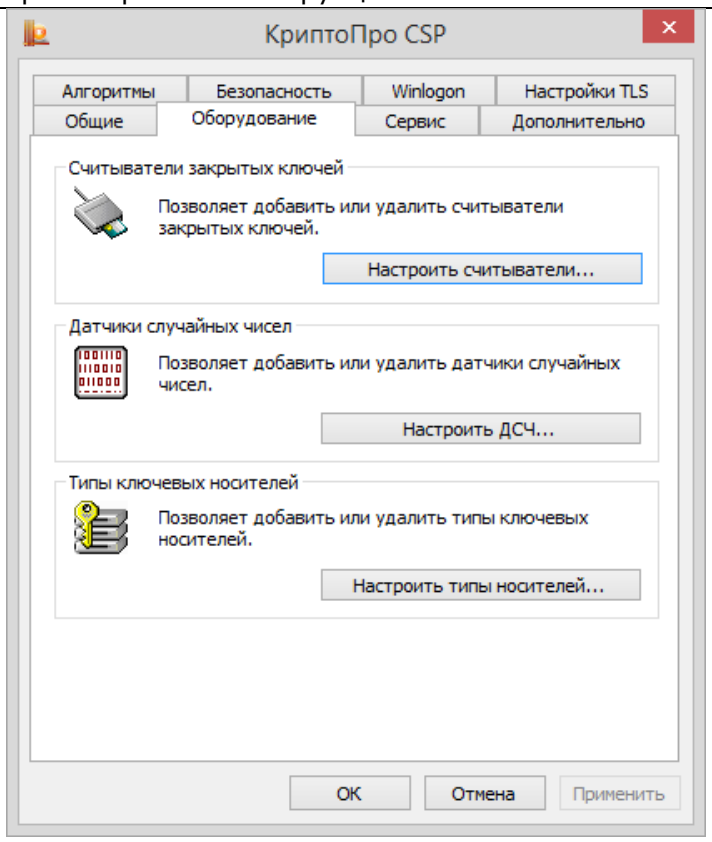


Рисунок 16. Контрольная панель. Вкладка «Оборудование»

Откроется окно «Управление считывателями» (см. Рисунок 17).

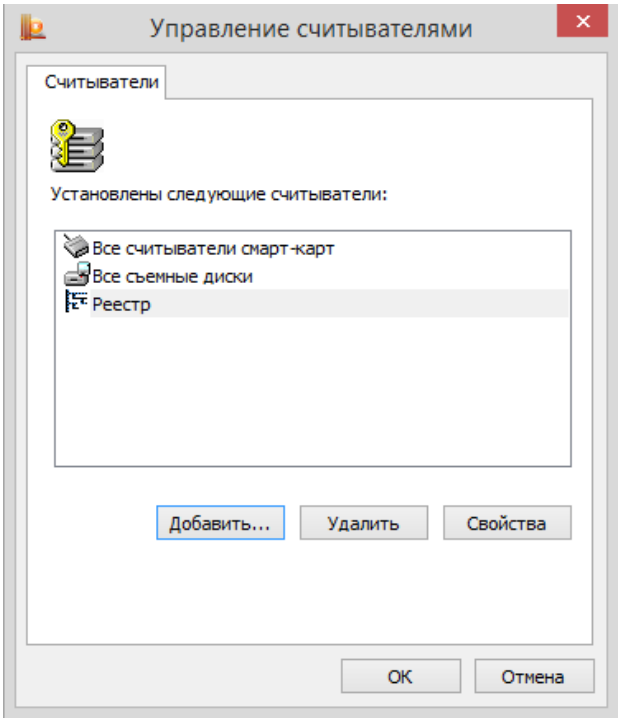


Рисунок 17. Окно «Управление считывателями»

Для того чтобы в КриптоПро CSP стало доступным использование нового считывателя, нажмите кнопку **Добавить**. Запустится мастер установки считывателя (см. Рисунок 18).

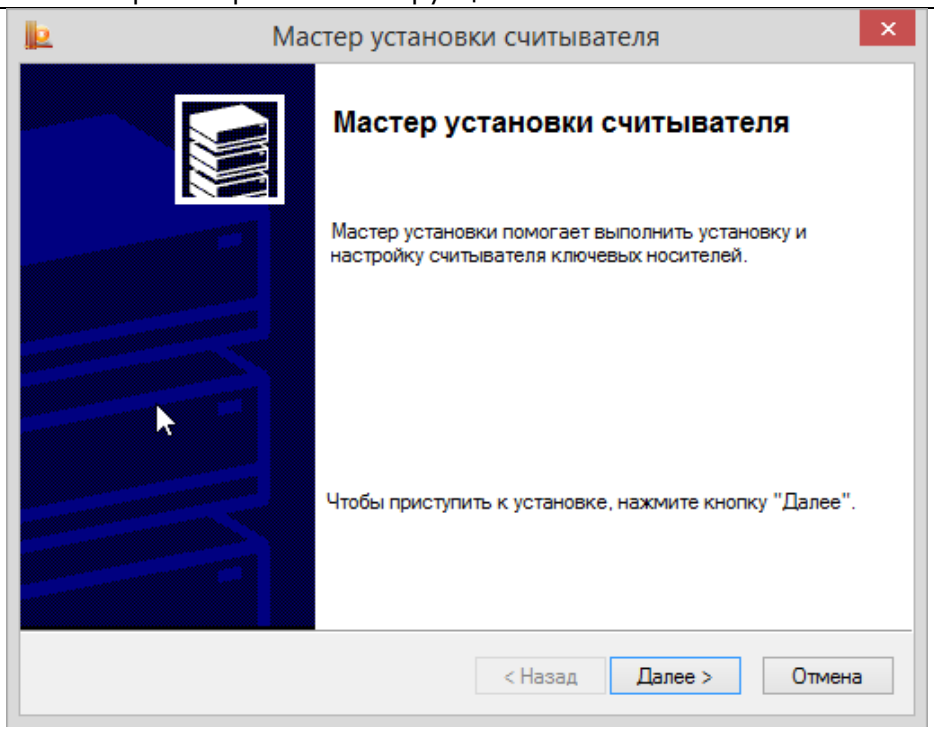


Рисунок 18. Запуск мастера установки считывателя

Нажмите кнопку **Далее**, чтобы перейти к шагу «Выбор считывателя» (см. Рисунок 19). Выберите из списка считыватель, который следует добавить.

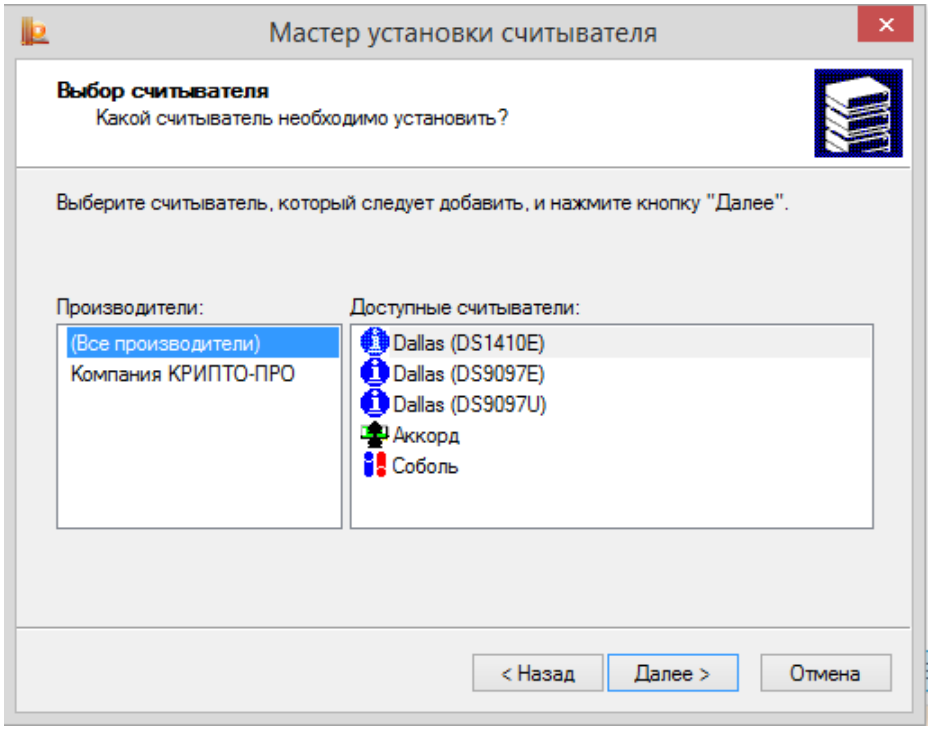


Рисунок 19. Окно «Выбор считывателя»

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 20). В этом окне выберите соединение для считывателя и нажмите кнопку **Далее.**

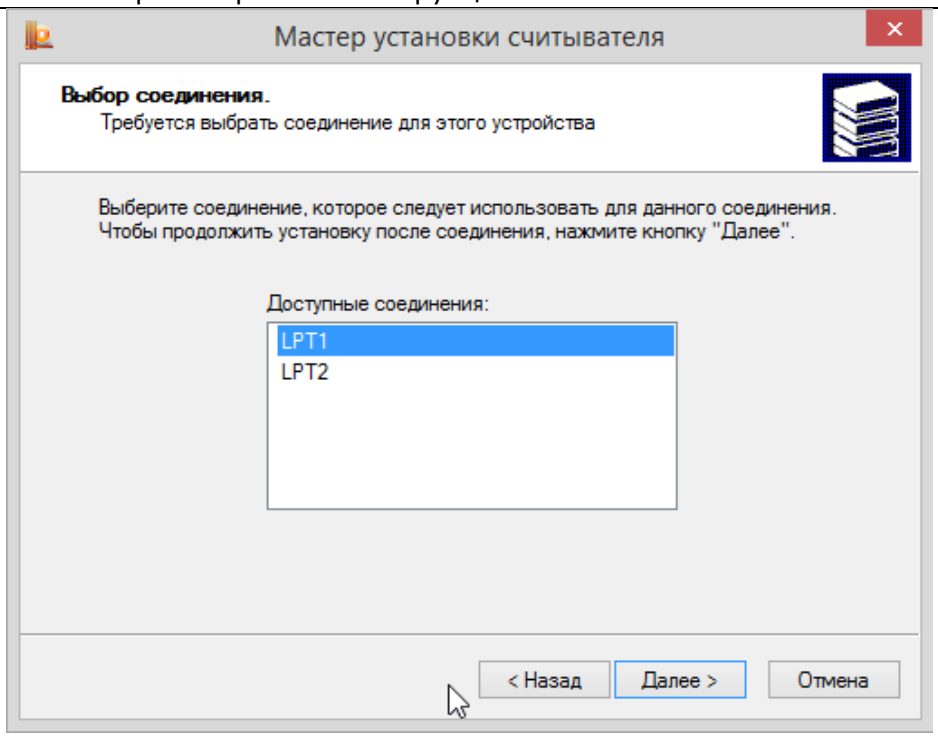


Рисунок 20. Окно «Выбор соединения»

На следующем шаге выводится окно «Имя считывателя» (см. Рисунок 21). В этом окне введите имя выбранного считывателя и нажмите кнопку **Далее.**

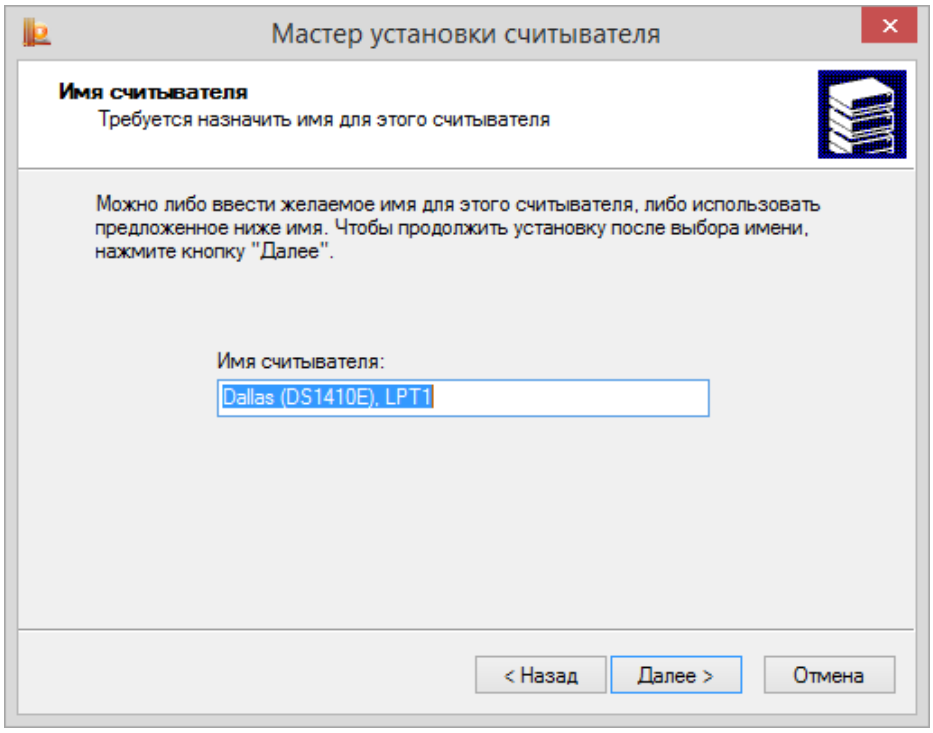


Рисунок 21. Окно «Имя считывателя»

Последний шаг - «Завершение работы мастера установки считывателя» (см. Рисунок 22). Внимательно прочитайте текст в этом окне, нажмите кнопку **Готово** и перезагрузите компьютер, если это требуется.

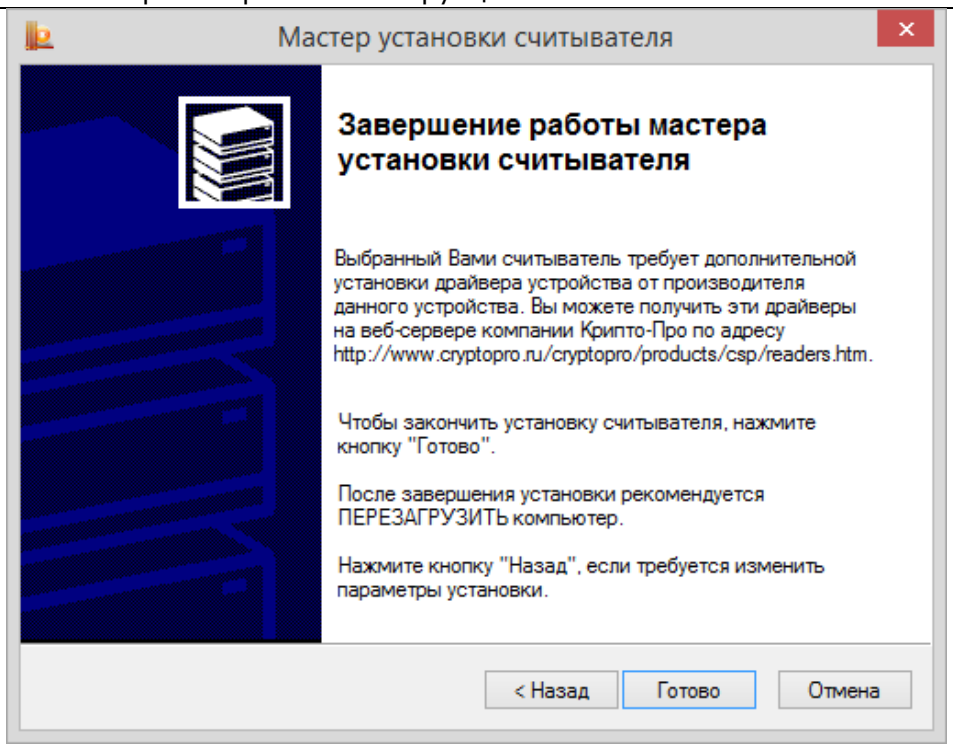


Рисунок 22. Завершение мастера установки считывателя

Примечание. Имеется возможность установки драйверов сторонних производителей, обеспечивающие 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 установлено, и нужно использовать новые устройства, необходимо установить поддерживающие драйвера и другие модули от производителей этих устройств.

2.4.1.2. Удаление считывателя

Для того, чтобы удалить считыватель, 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить считыватели.**

Откроется окно «Управление считывателями» (см. Рисунок 17). Выберите считыватель, который требуется сделать недоступным, и нажмите кнопку **Удалить.**

В открывшемся диалоге подтвердите удаление считывателя, нажав **ОК**.

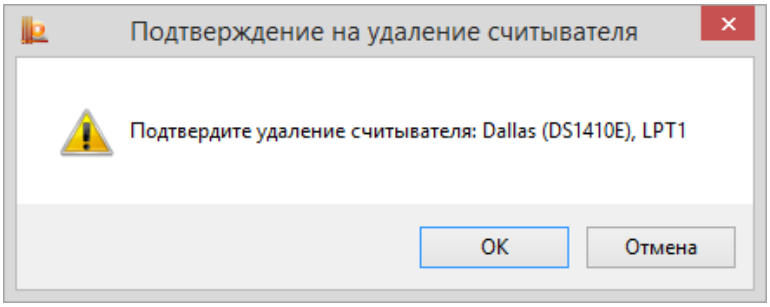


Рисунок 23. Окно «Подтверждение на удаление считывателя»

После подтверждения использование считывателя СКЗИ станет недоступно.

2.4.1.3. Просмотр свойств считывателя

Чтобы просмотреть свойства считывателя откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рисунок 16) нажмите кнопку **Настроить считыватели.**

Откроется окно «Управление считывателями» (см. Рисунок 17). Выберите считыватель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Выведется справочная информация о выбранном считывателе, в том числе, и данные о состоянии устройства. После просмотра свойств считывателя нажмите кнопку **ОК.**

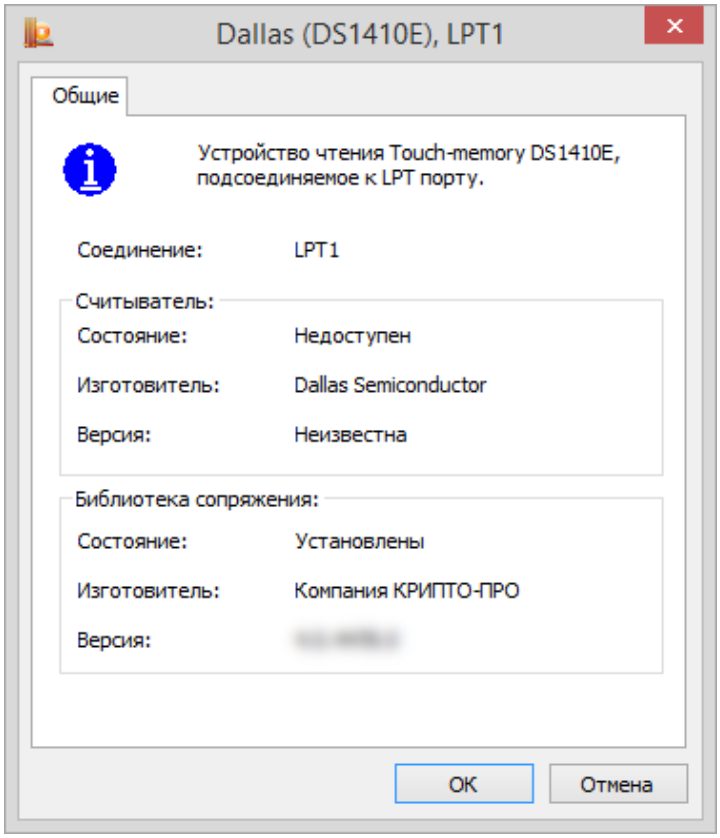


Рисунок 24. Свойства считывателя

2.4.2. Изменение набора устройств хранения ключевой информации

2.4.2.1. Добавление носителя

Для того, чтобы сделать доступным носитель 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей.**

Откроется окно «Управление ключевыми носителями» (см. Рисунок 25).

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

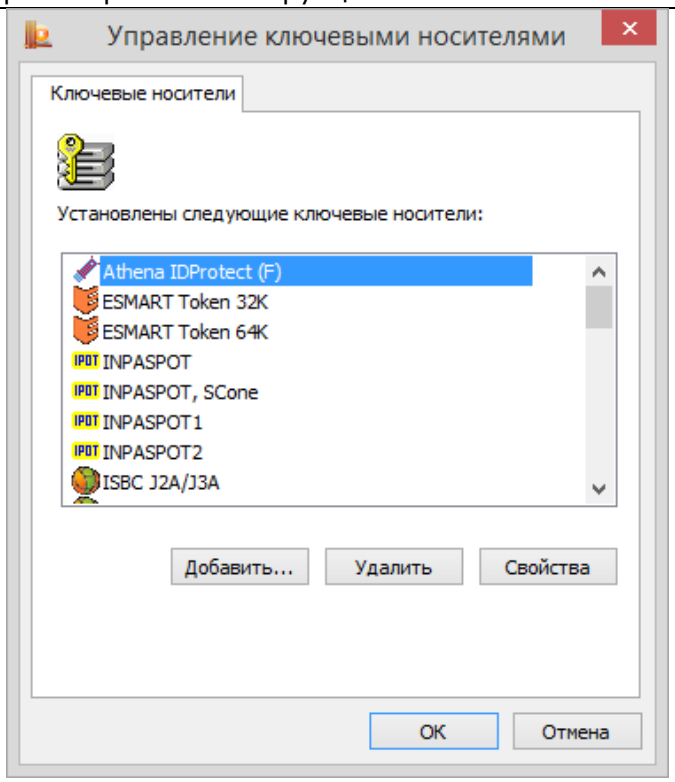


Рисунок 25. Окно «Управление ключевыми носителями»

Для того, чтобы сделать доступным ключевой носитель, нажмите кнопку **Добавить**. Запустится мастер установки ключевого носителя (см. Рисунок 26).

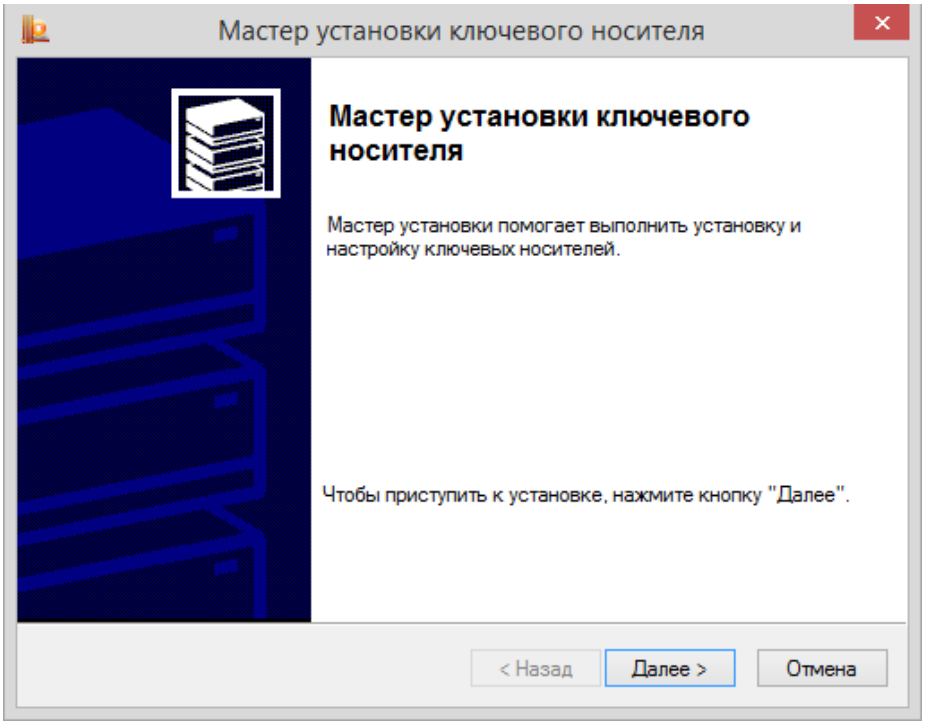


Рисунок 26. Запуск мастера установки ключевого носителя

Нажмите кнопку **Далее**, чтобы перейти к шагу выбора ключевого носителя (см. Рисунок 27). Выберите ключевой носитель, который следует сделать доступным, и нажмите кнопку **Далее.**

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

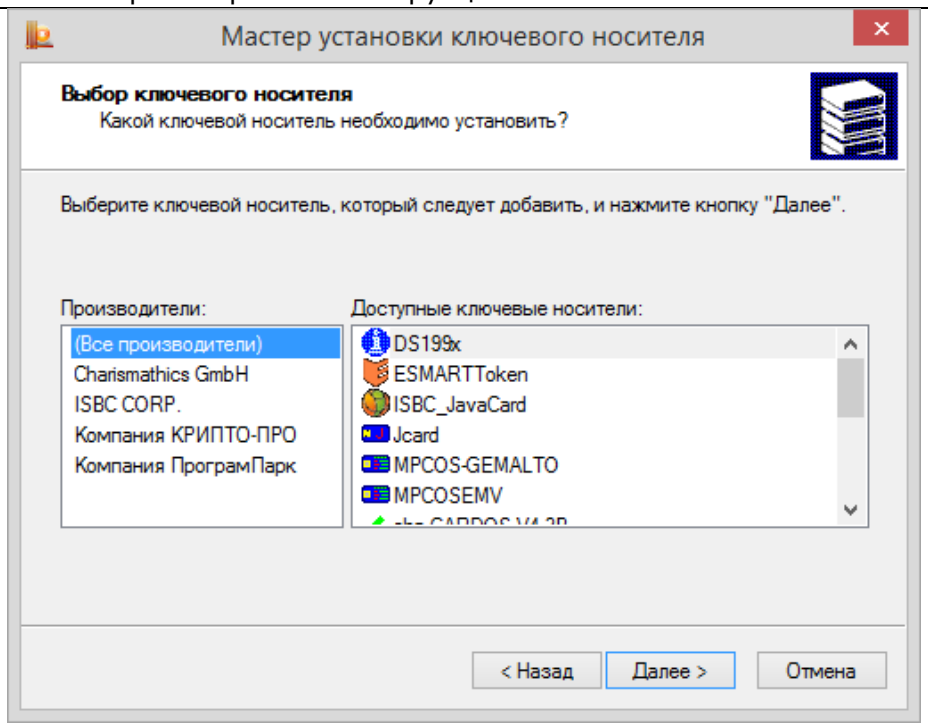


Рисунок 27. Окно «Выбор ключевого носителя»

После выбора ключевого носителя откроется окно «Имя ключевого носителя» (см. Рисунок 28). В этом окне введите имя выбранного носителя и нажмите кнопку **Далее.**

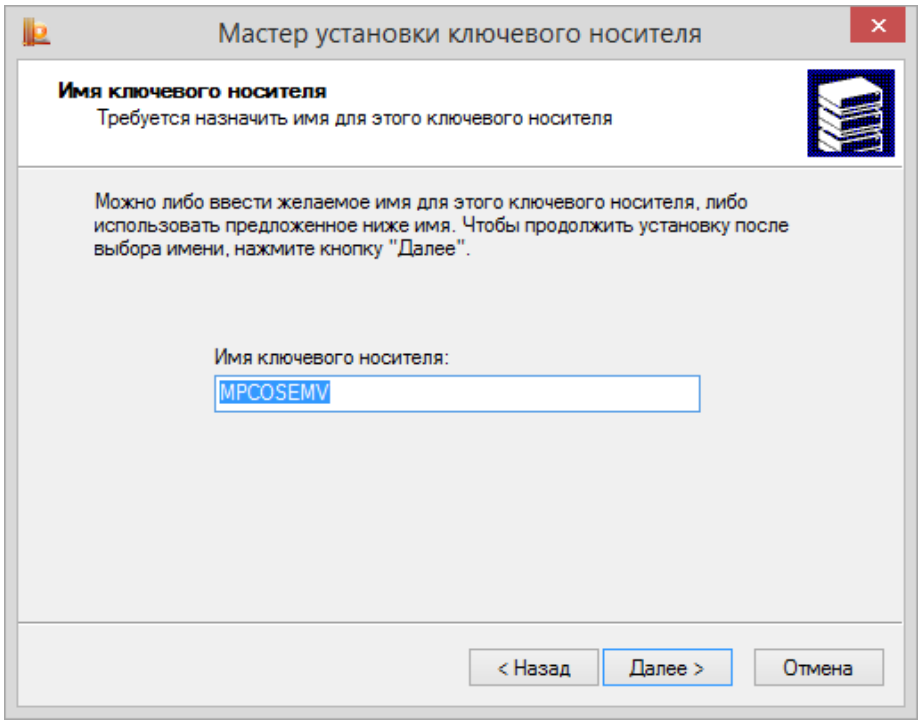


Рисунок 28. Окно «Имя ключевого носителя»

В зависимости от типа ключевого носителя следующие шаги мастера могут различаться, так для MPCOS/EMV будет отображено окно «Разметка карты» (см. Рисунок 29). В этом окне нужно указать разметку карты, после чего перейти к следующему шагу.

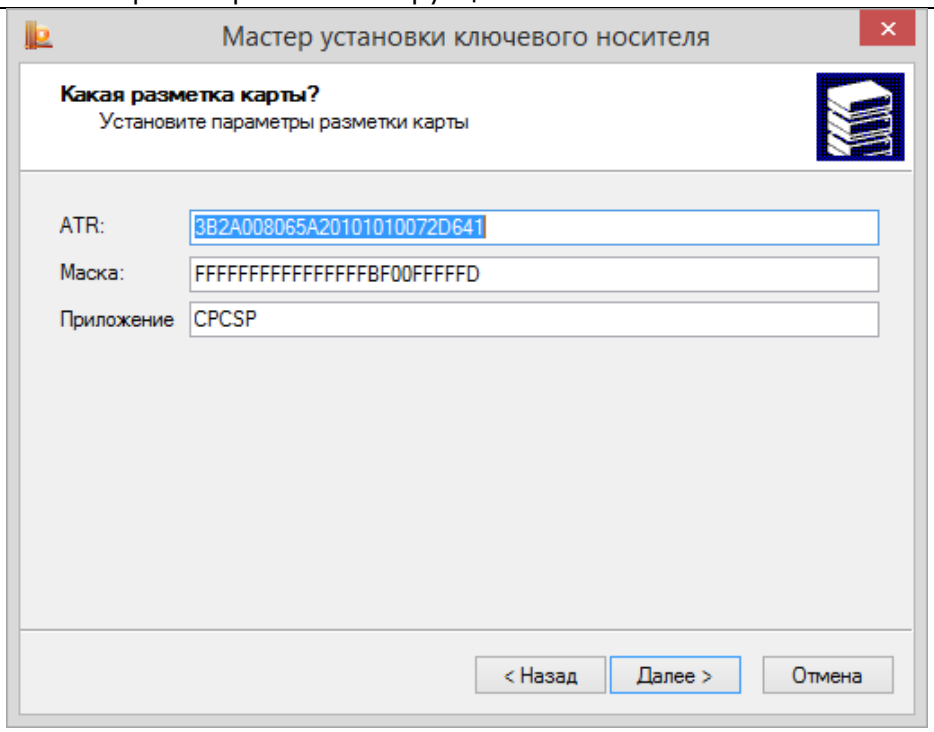


Рисунок 29. Окно «Разметка карты»

Откроется окно «Завершение работы мастера установки ключевого носителя» (см. Рисунок 30). Нажмите в нем кнопку **Готово**.

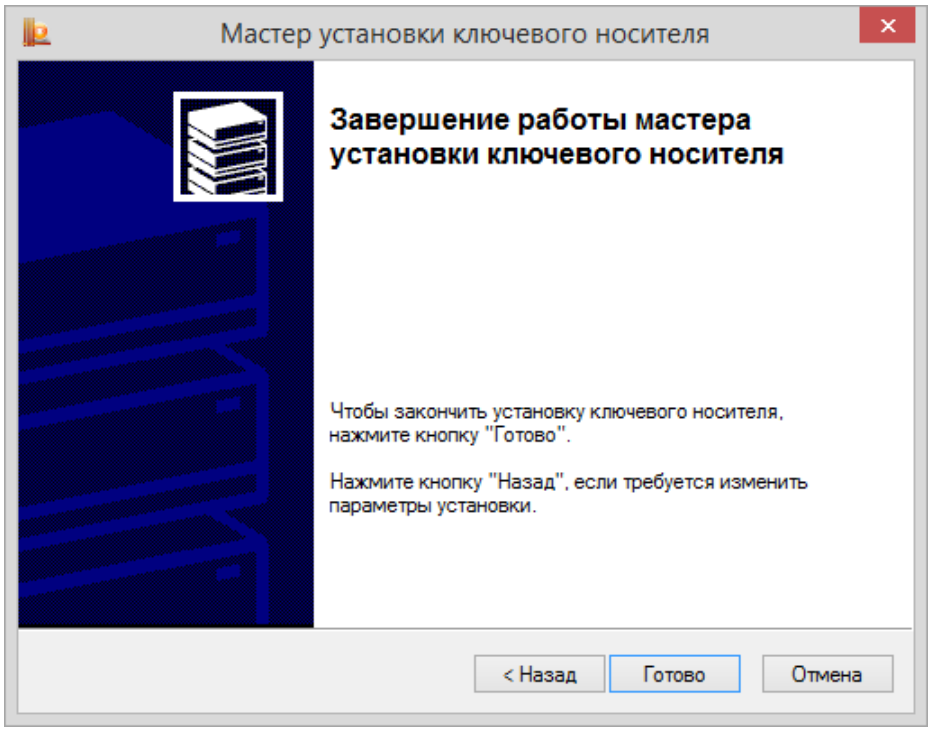


Рисунок 30. Завершение мастера установки ключевого носителя

Установленный ключевой носитель отобразится в списке окна «Управление ключевыми носителями (см. Рисунок 25).

2.4.2.2. Удаление ключевого носителя

Для того чтобы сделать недоступным ключевой носитель 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить типы носителей.**

В открывшемся диалоге подтвердите удаление ключевого носителя, нажав **ОК**.

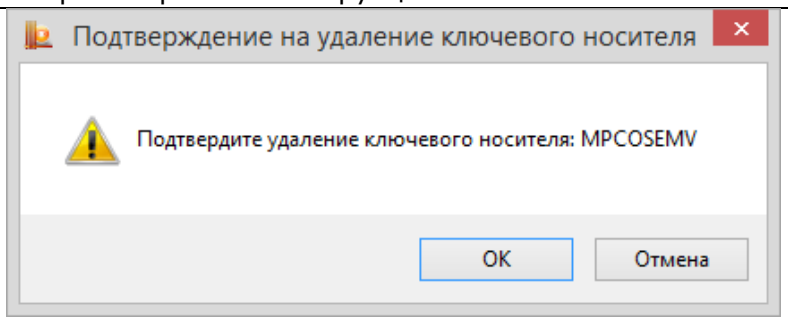


Рисунок 31. Окно «Подтверждение на удаление ключевого носителя»

После подтверждения ключевой носитель станет недоступен для использования в работе криптопровайдера.

2.4.2.3. Просмотр свойств ключевого носителя

Для того, чтобы просмотреть свойства ключевого носителя, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Оборудование**. В панели настройки оборудования СКЗИ КриптоПро CSP (см. Рисунок 16) нажмите кнопку **Настроить типы носителей.**

В открывшемся окне «Управление ключевыми носителями» (см. Рисунок 25) выберите ключевой носитель, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Откроется окно «Свойства: Имя носителя» (см. Рисунок 32), в котором отображается справочная информация о выбранном ключевом носителе, в том числе, и данные о состоянии устройства. После просмотра свойств ключевого носителя нажмите кнопку **OK.**

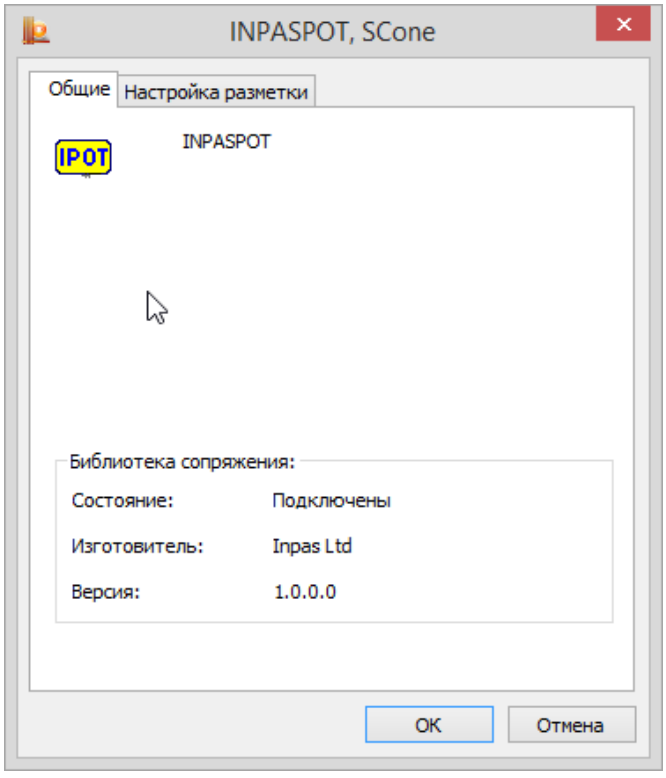


Рисунок 32. Окно «Свойства: имя носителя»

2.4.3. Настройка датчиков 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 того чтобы добавить 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ.**

Откроется окно «Управление датчиками случайных чисел» (см. Рисунок 33).

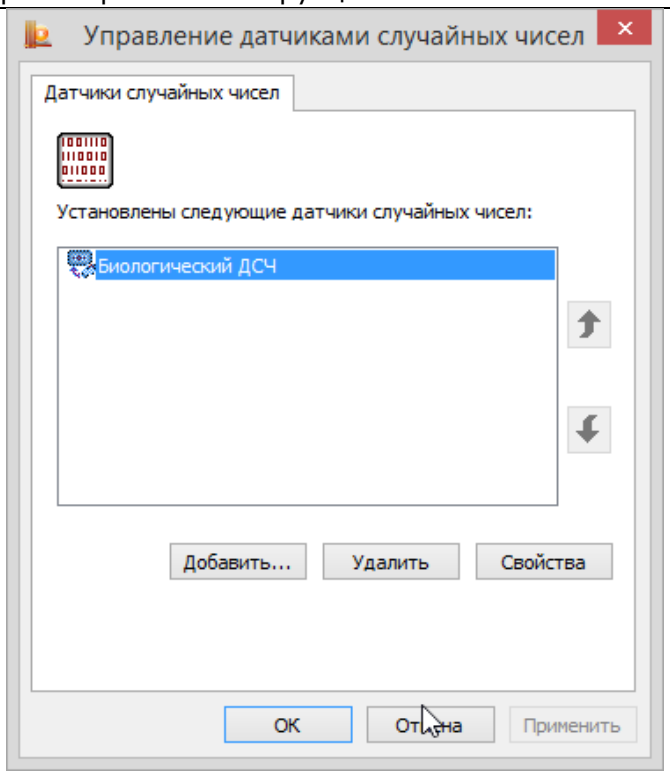


Рисунок 33. Окно «Управление датчиками случайных чисел»

Для того, чтобы добавить ДСЧ, нажмите кнопку **Добавить**. Запустится мастер установки ДСЧ (см. Рисунок 34). Нажмите кнопку **Далее**, чтобы перейти к следующему шагу.

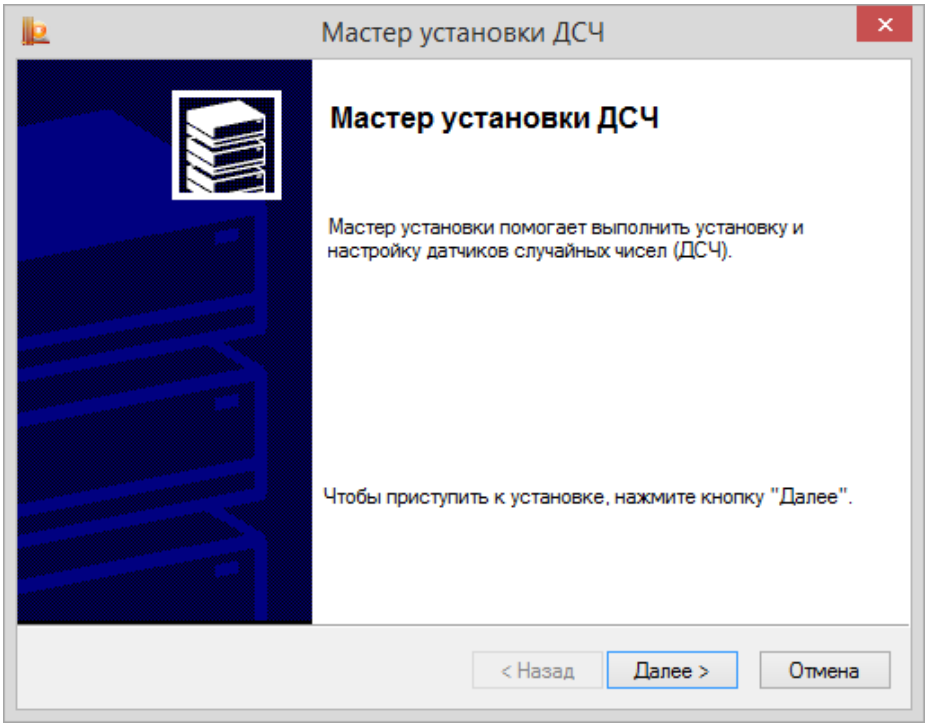


Рисунок 34. Запуск мастера установки ДСЧ

Откроется окно «Выбор ДСЧ» (см. Рисунок 35). В этом окне выберите датчик случайных чисел, который требуется добавить, и нажмите кнопку **Далее**, чтобы перейти к следующему шагу.

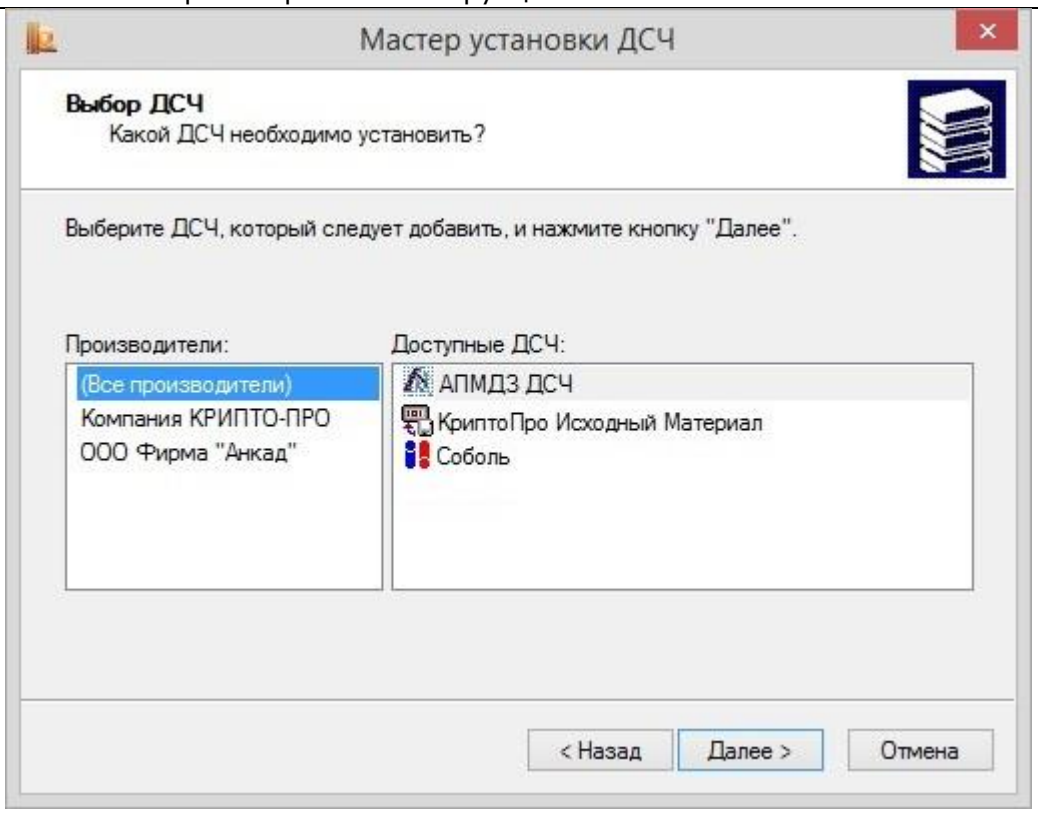


Рисунок 35. Окно «Выбор ДСЧ»

Откроется окно «Имя ДСЧ» (см. Рисунок 36). В этом окне введите имя выбранного датчика случайных чисел и нажмите кнопку **Далее.**

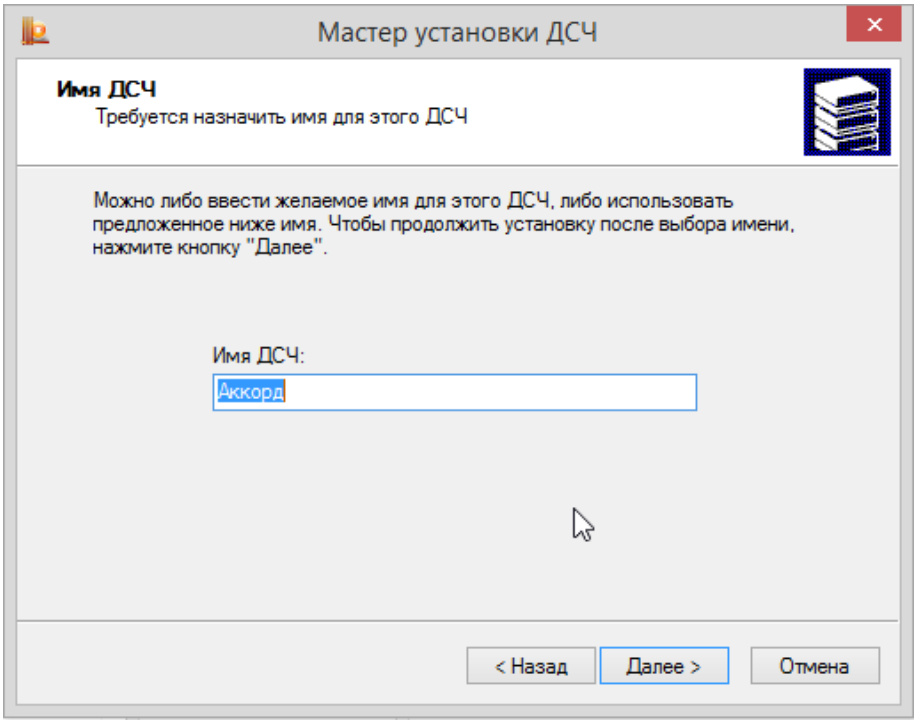


Рисунок 36. Окно «Имя ДСЧ»

Последним шагом мастера откроется окно «Завершение работы мастера установки ДСЧ» (см. Рисунок 37). Нажмите в нем кнопку **Готово** и перезагрузите компьютер**.**

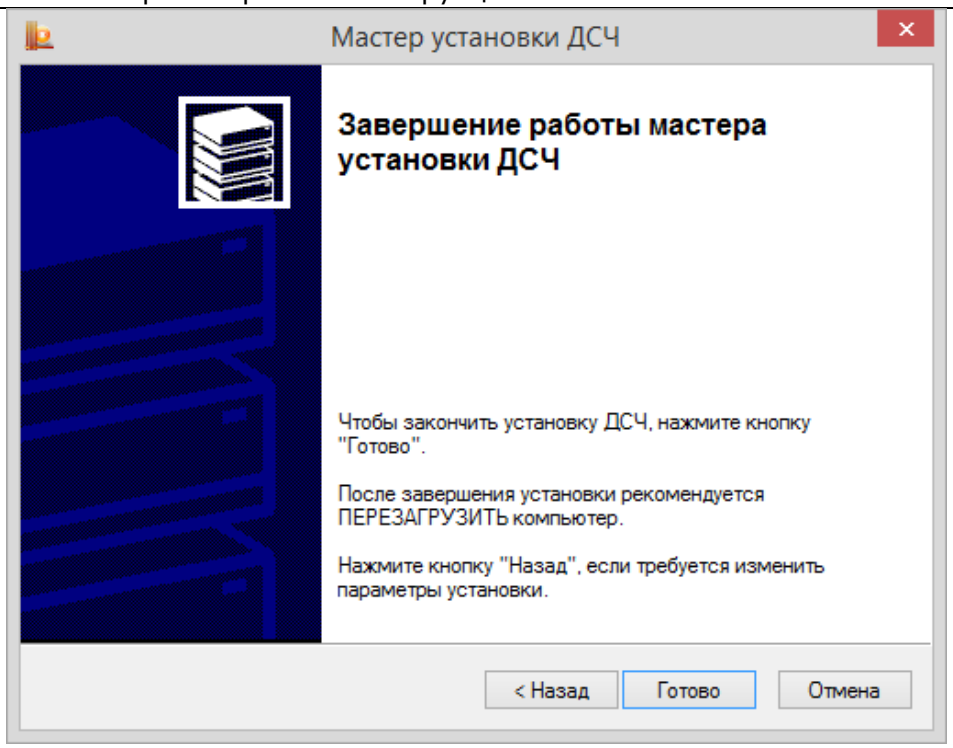


Рисунок 37. Завершение мастера установки ДСЧ

2.4.3.2. Удаление ДСЧ

Для того, чтобы удалить 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

В открывшемся окне «Управление датчиками случайных чисел» (см. Рисунок 33) выберите датчик, который требуется удалить, и нажмите кнопку **Удалить.**

В появившемся диалоге нажмите **ОК**.

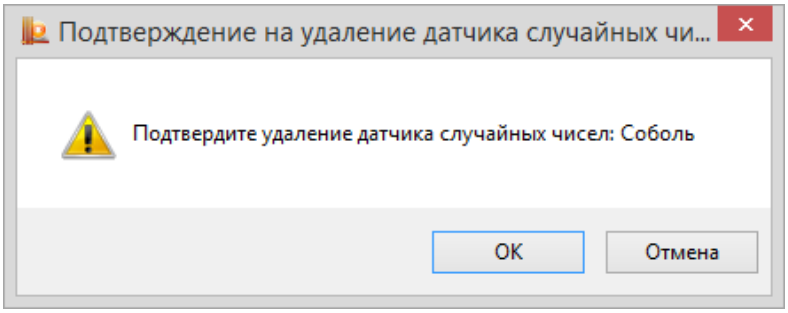


Рисунок 38. Окно «Подтверждение на удаление ДСЧ»

После подтверждения ДСЧ будет удалён.

2.4.3.3. Просмотр свойств ДСЧ

Для того чтобы просмотреть свойства ДСЧ, Для того чтобы добавить 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 11). После перезапуска перейдите на вкладку **Оборудование** и нажмите кнопку **Настроить ДСЧ**.

Откроется окно «Управление датчиками случайных чисел» (см. Рисунок 33). Выберите датчик, свойства которого требуется просмотреть, и нажмите кнопку **Свойства.**

Откроется окно «Свойства: Имя ДСЧ» (см. Рисунок 39), в котором отображается справочная информация о выбранном датчике случайных чисел, в том числе и данные о состоянии устройства. После просмотра свойств ДСЧ нажмите кнопку **ОК.**

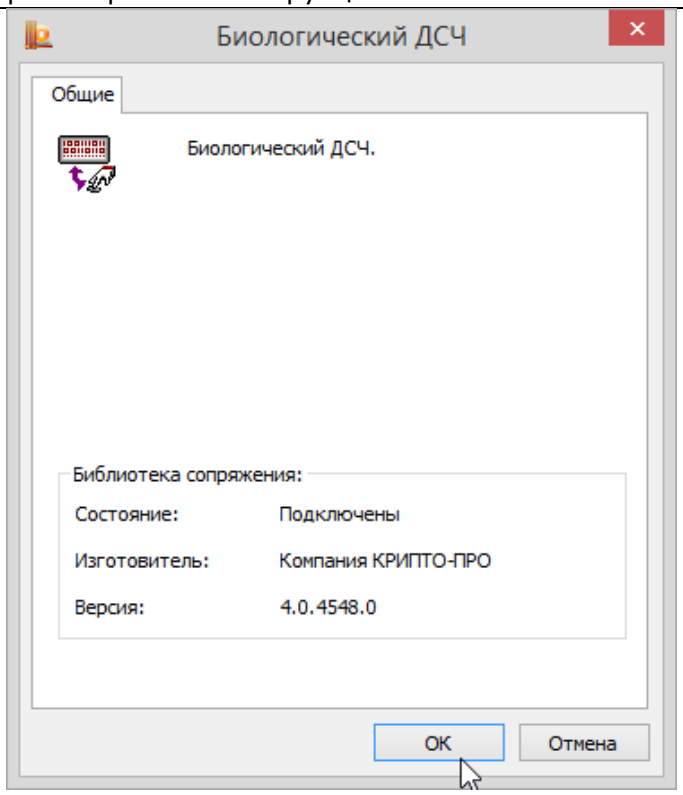


Рисунок 39. Окно «Свойства: имя ДСЧ»

Примечание. Если в СКЗИ настроено несколько датчиков случайных чисел, 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 датчиков случайных чисел указан ДСЧ Электронного замка «Соболь», то формирование исходной ключевой информации будет осуществляться на ДСЧ Электронного замка «Соболь».

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

2.5. Работа с контейнерами и сертификатами

Вкладка **Сервис** контрольной панели 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;
- Очистка информации о ранее использованных съёмных носителях, на которых располагались контейнеры закрытых ключей.

2.5.1. Тестирование, копирование и удаление контейнера закрытого ключа

2.5.1.1. Тестирование контейнера закрытого ключа

Для того чтобы провести тест работоспособности контейнера закрытого ключа, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40). Нажмите кнопку **Протестировать.**

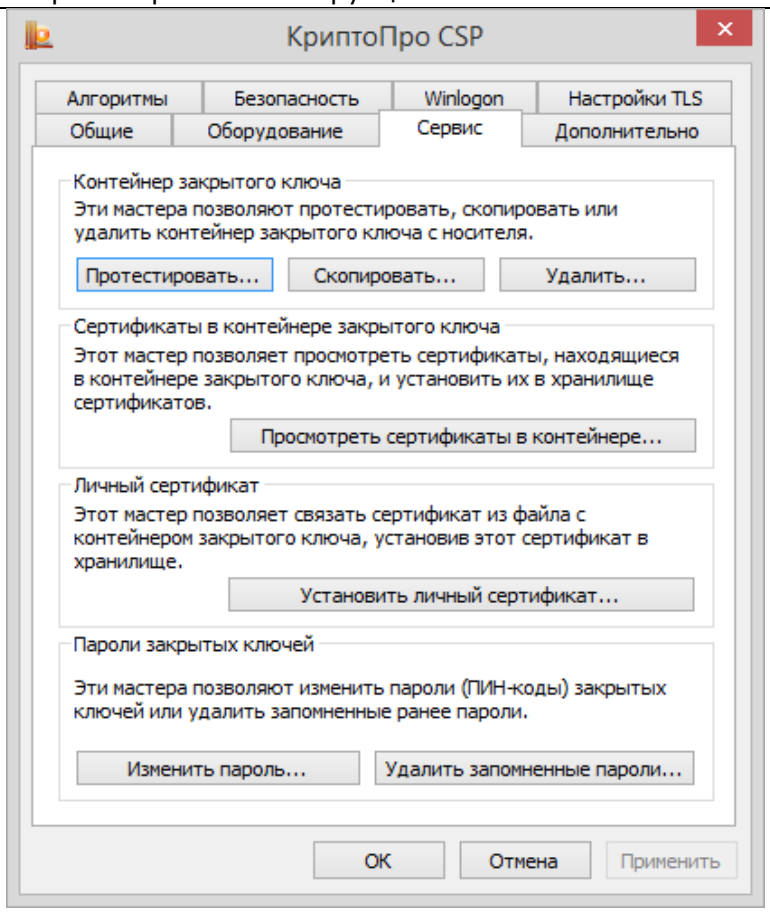


Рисунок 40. Контрольная панель. Вкладка «Сервис»

Откроется окно «Тестирование контейнера закрытого ключа» (см. Рисунок 41).

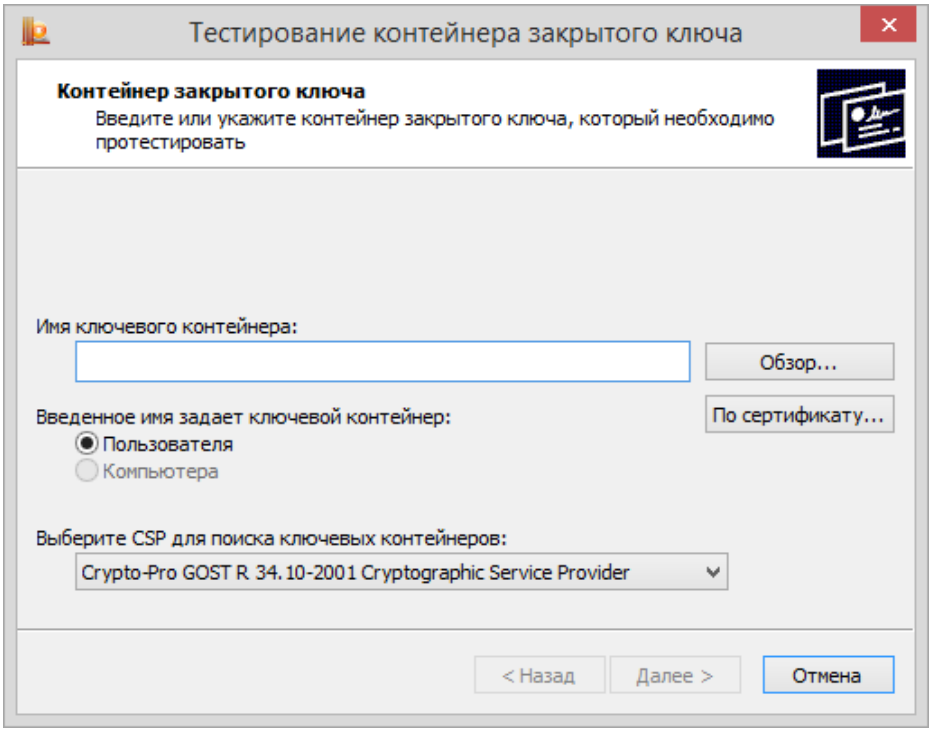


Рисунок 41. Окно «Тестирование контейнера закрытого ключа»

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

Опции поиска:

- **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.

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

После этого откроется форма с результатом тестирования (см. Рисунок 42), в котором будет выведена информация о данном контейнере и результат теста.

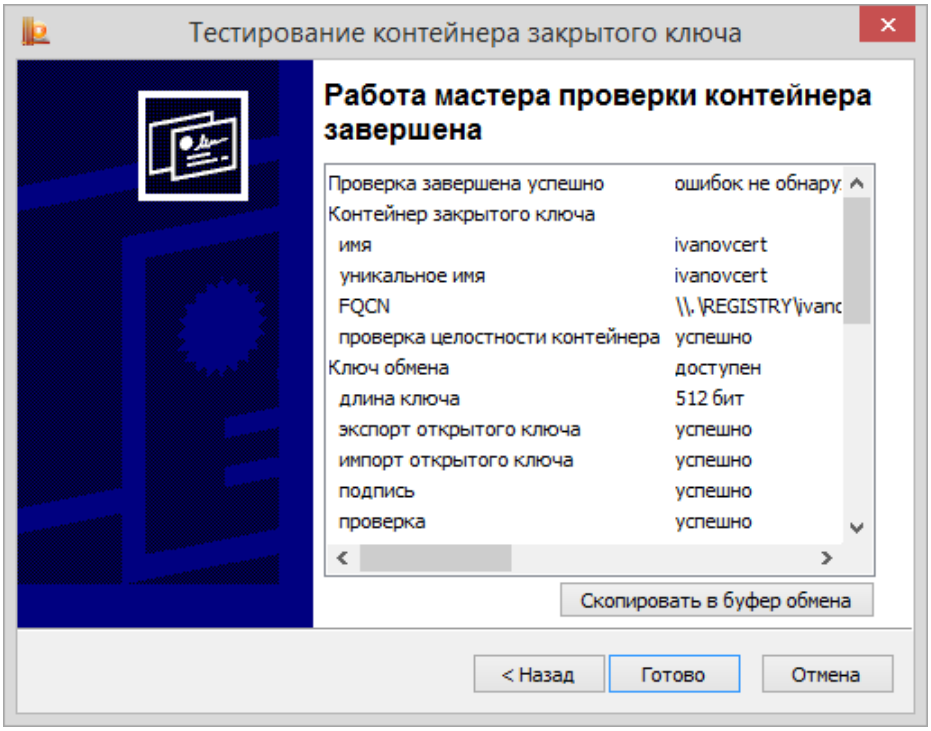


Рисунок 42. Итоговое окно «Тестирование контейнера закрытого ключа»

2.5.1.2. Копирование контейнера закрытого ключа

Для того чтобы скопировать контейнер закрытого ключа, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40). Нажмите кнопку **Скопировать**.

Откроется окно «Копирование контейнера закрытого ключа» (см. Рисунок 43).

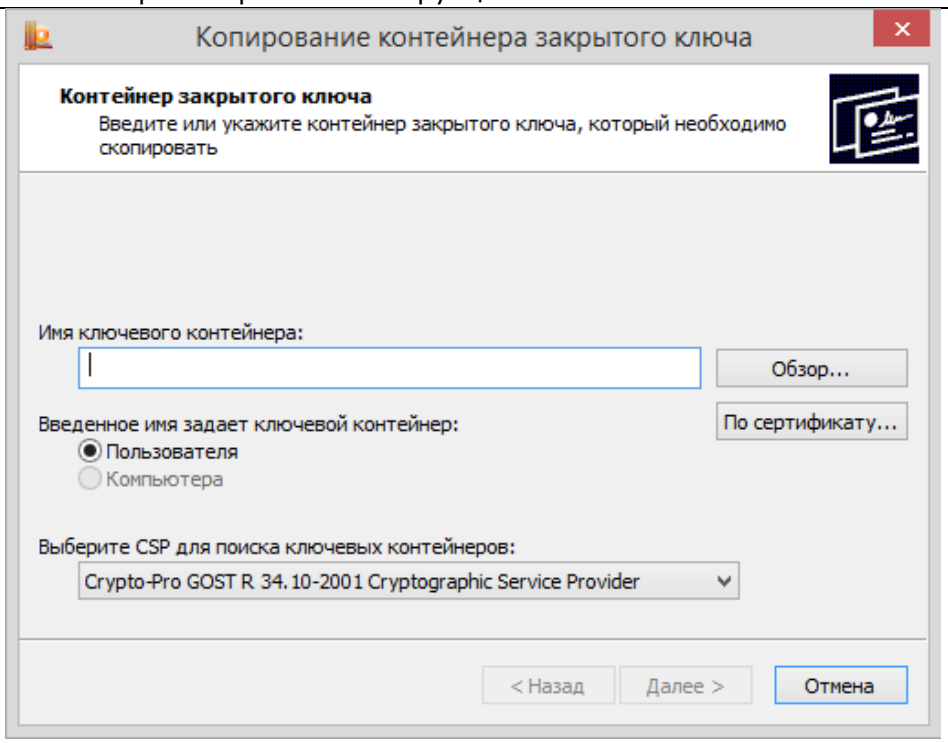


Рисунок 43. Окно «Копирование контейнера закрытого ключа»

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

Опции поиска:

- **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 того, как все поля заполнены, нажмите кнопку **Далее**.

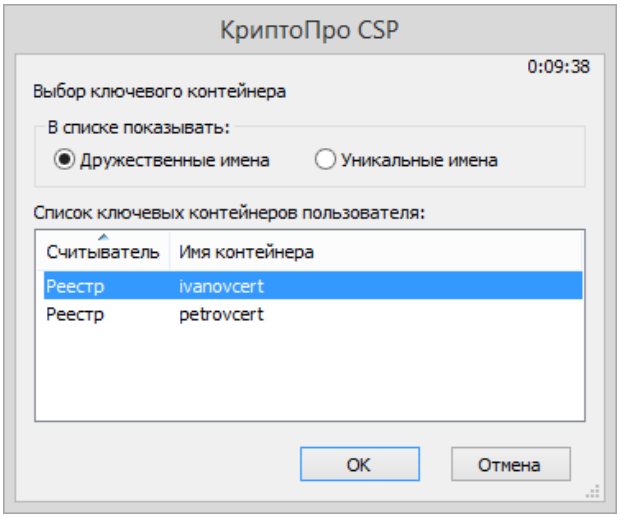


Рисунок 44. Выбор ключевого контейнера

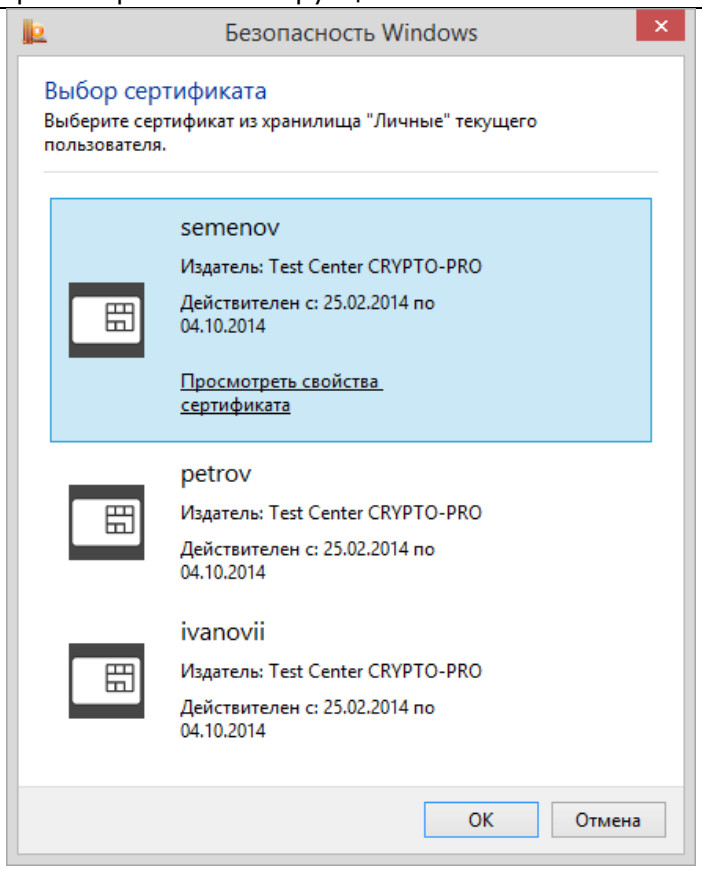


Рисунок 45. Выбор сертификата

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

Откроется окно ввода параметров нового контейнера закрытого ключа (см. Рисунок 46). 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.

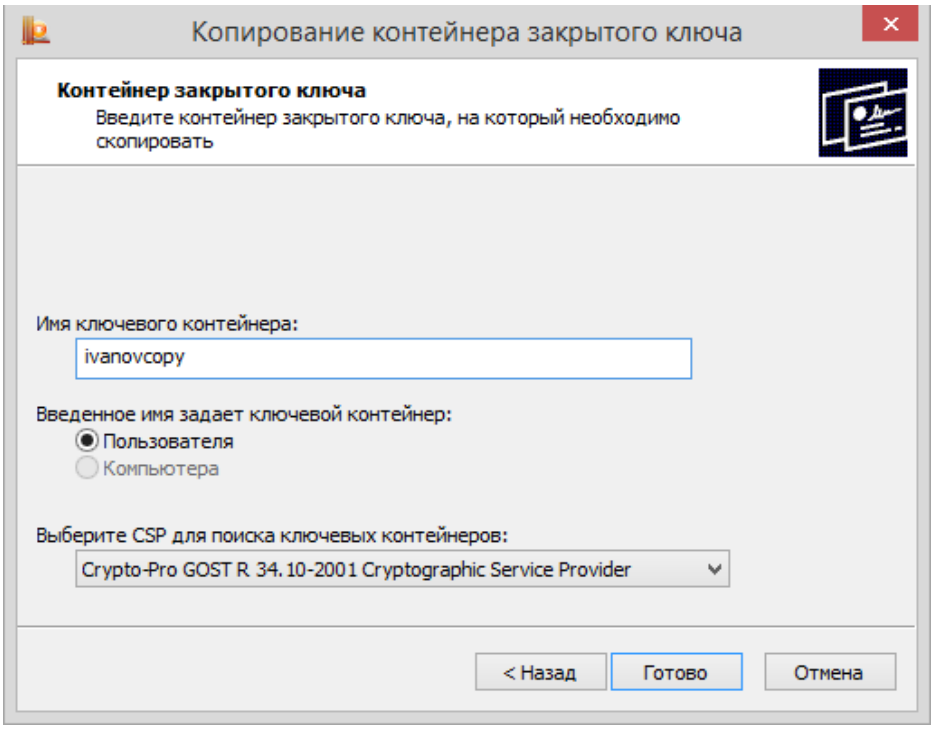


Рисунок 46. Окно «Копирование контейнера закрытого ключа»

После ввода нажмите кнопку **Готово**. Откроется окно, в котором необходимо выбрать носитель для скопированного контейнера (см. Рисунок 47).

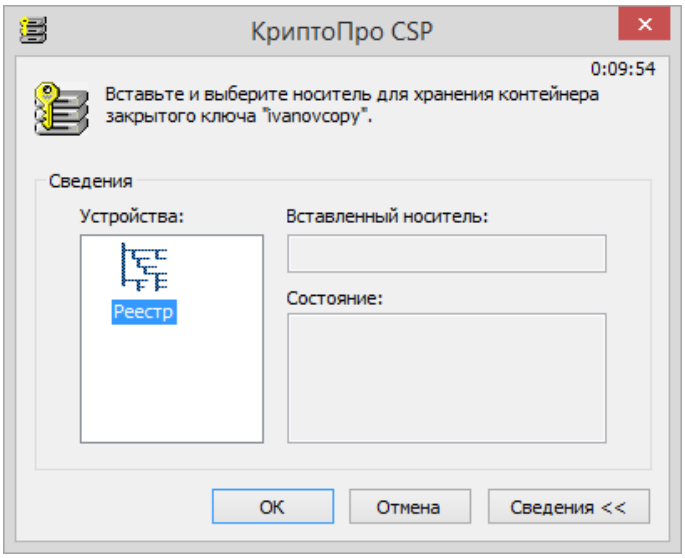


Рисунок 47. Окно выбора носителя

Вставьте носитель в считыватель, выберите носитель из перечня устройств и нажмите кнопку **ОК**. Откроется окно создания пароля на доступ к закрытому ключу (см. Рисунок 48). Введите пароль, подтвердите его.

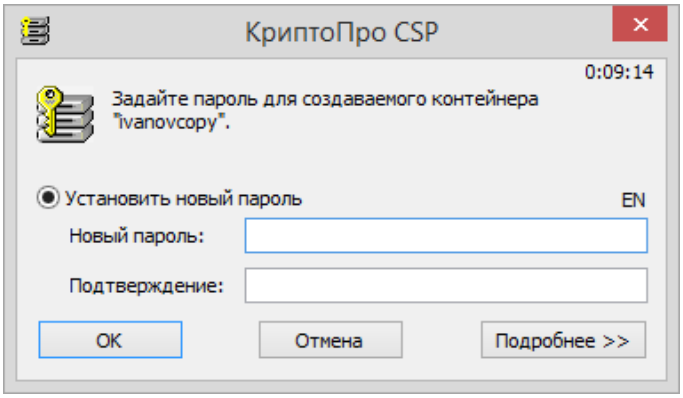


Рисунок 48. Окно ввода пароля

После ввода необходимых данных нажмите кнопку **ОК**. СКЗИ «КриптоПро CSP» осуществит копирование контейнера закрытого ключа.

2.5.1.3. Удаление контейнера закрытого ключа

Для того чтобы удалить контейнер закрытого ключа откройте Панель управления СКЗИ КриптоПро CSP, перейдите на вкладку **Сервис** (см. Рисунок 40) и нажмите кнопку **Удалить контейнер**.

Откроется окно «Удаление контейнера закрытого ключа» (см. Рисунок 49).

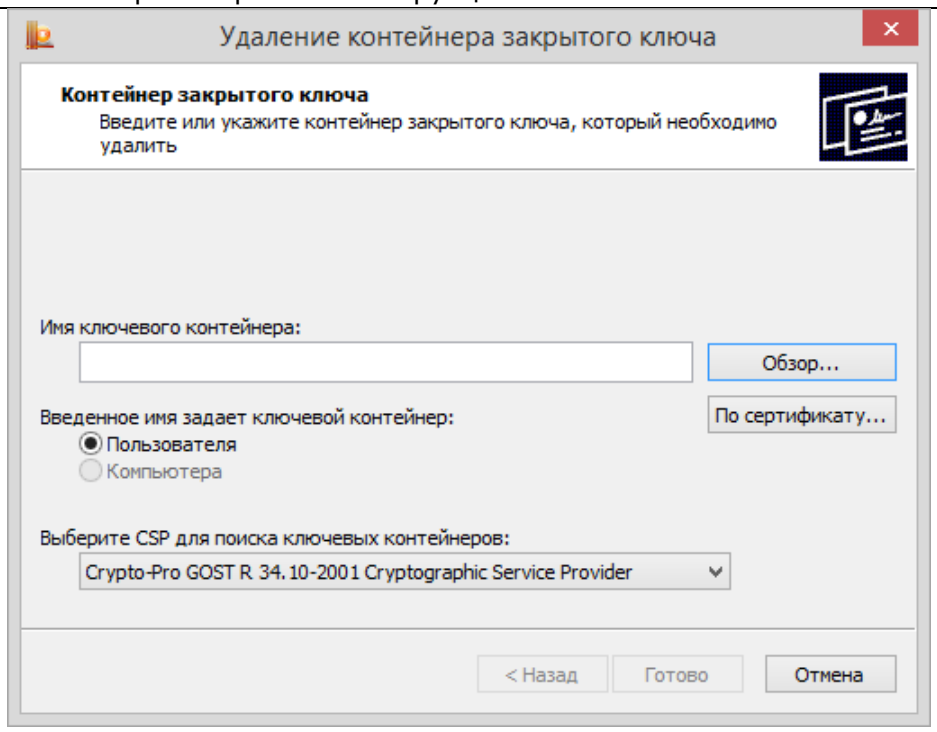


Рисунок 49. Окно «Удаление контейнера закрытого ключа»

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

Опции поиска:

- **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 того, как все поля заполнены, нажмите кнопку **Готово**.

В диалоге подтверждения удаления ключевого контейнера (см. Рисунок 50) нажмите кнопку **Да**.

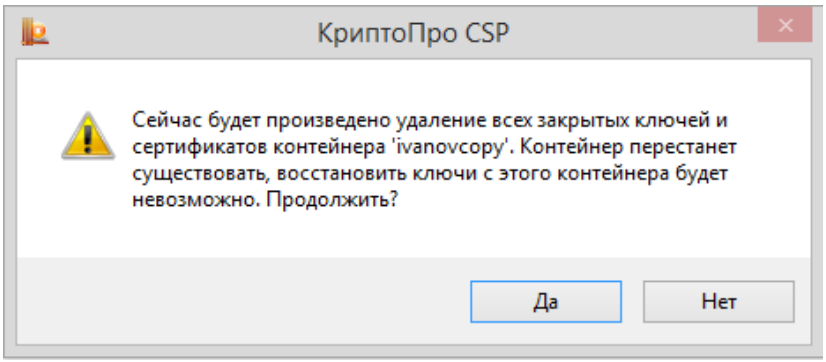


Рисунок 50. Окно подтверждения удаления ключевого контейнера

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 того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Просмотреть сертификаты в контейнере**.

Откроется окно «Сертификаты в контейнере закрытого ключа» (см. Рисунок 51).

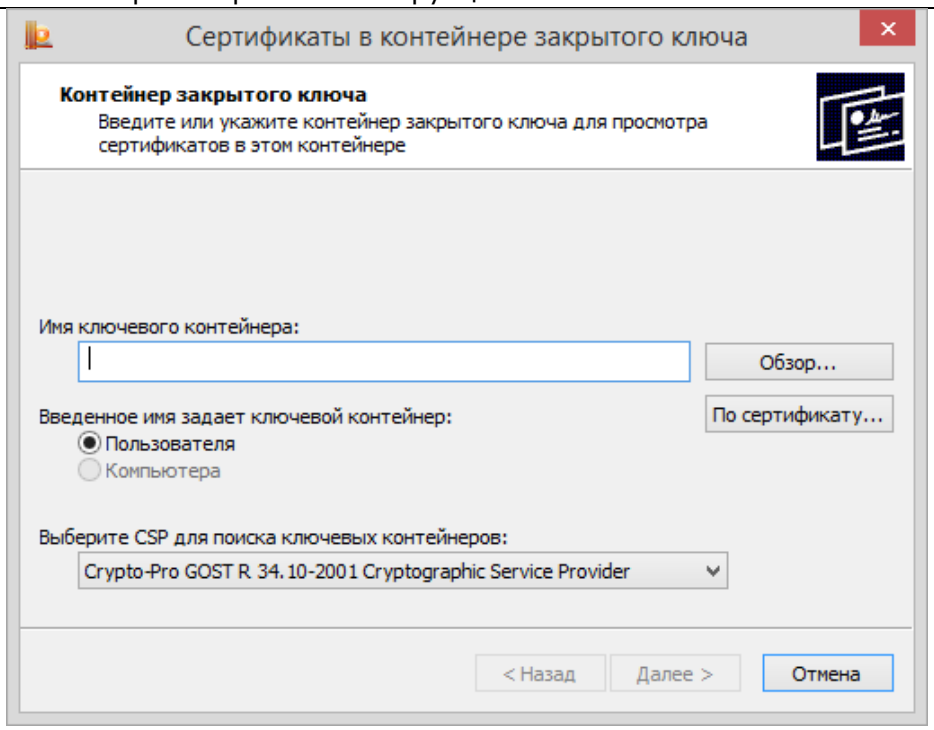


Рисунок 51. Окно «Сертификаты в контейнере закрытого ключа»

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

Опции поиска:

- **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 того, как все поля заполнены, нажмите кнопку **Далее**.

Если сертификата в контейнере закрытого ключа нет, об этом появится сообщение (см. Рисунок 52).

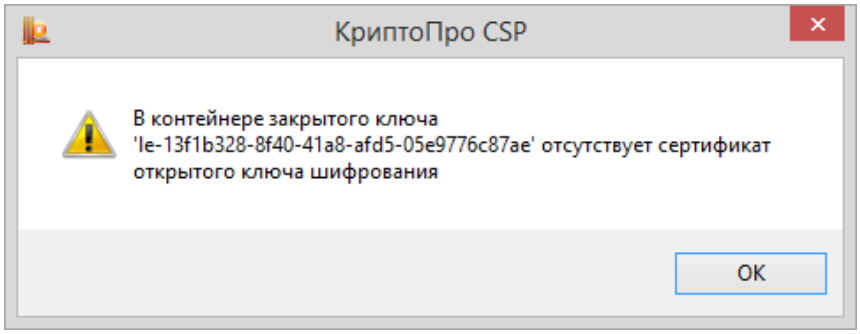


Рисунок 52. Окно, информирующее об отсутствии сертификата

Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра» (см. Рисунок 53).

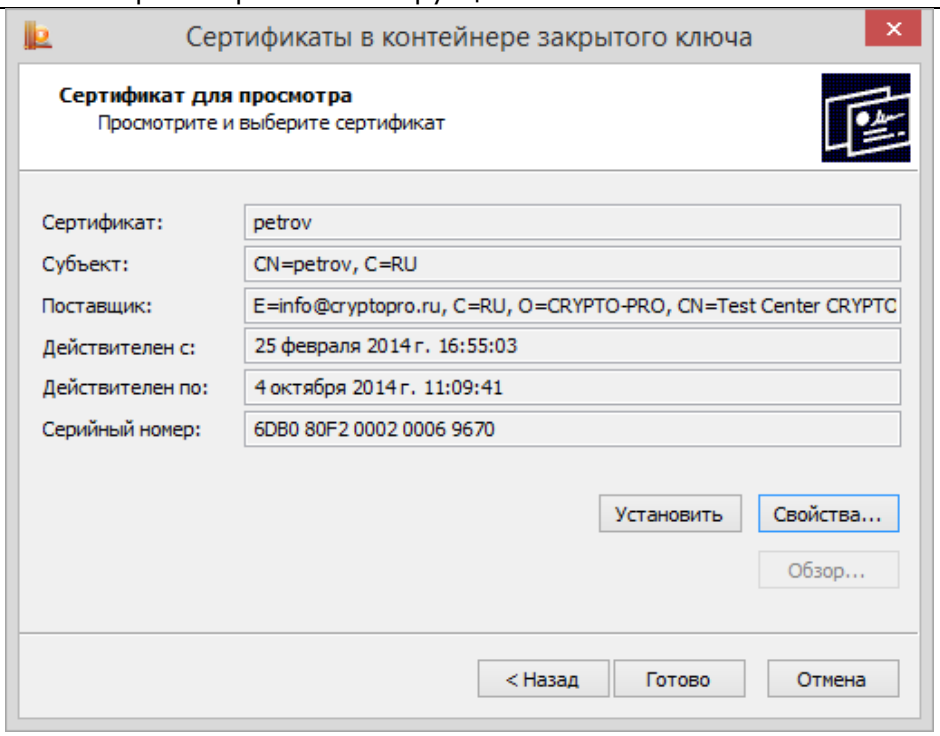


Рисунок 53. Окно «Сертификаты в контейнере закрытого ключа»

Для просмотра основных свойств сертификата нажмите кнопку **Свойства** в окне «Сертификаты в контейнере закрытого ключа» (см. Рисунок 53). Откроется окно просмотра свойств сертификата (см. Рисунок 54).

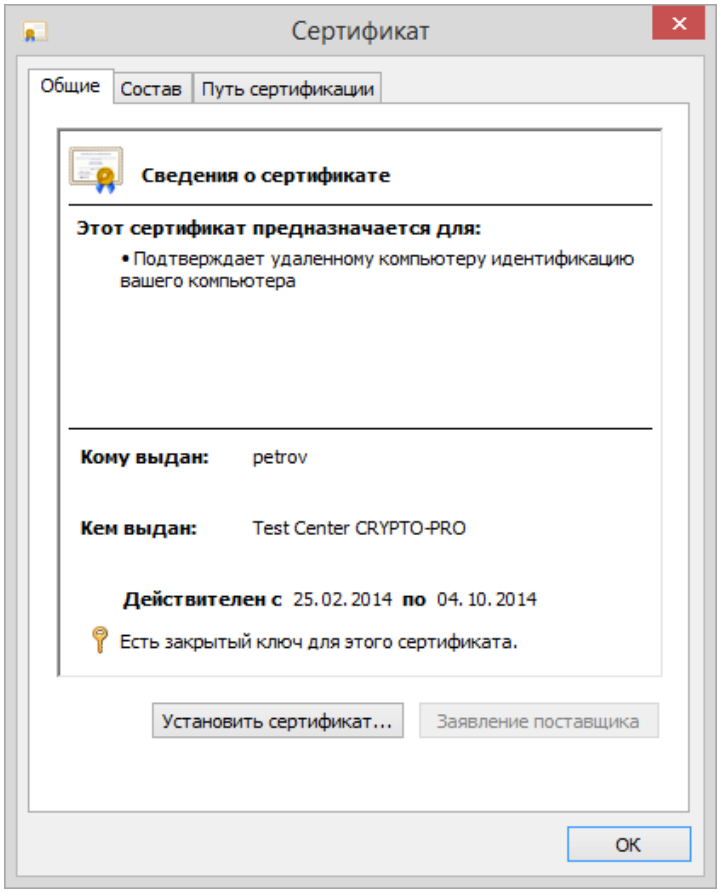


Рисунок 54. Окно просмотра свойств сертификата

На вкладке «Путь сертификации» можно просмотреть все сертификаты до корневого УЦ, если они содержатся в контейнере.

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 не только в локальном справочнике сертификатов компьютера, а также 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 того чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальный справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для того чтобы установить личный сертификат, 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 53) 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 55).

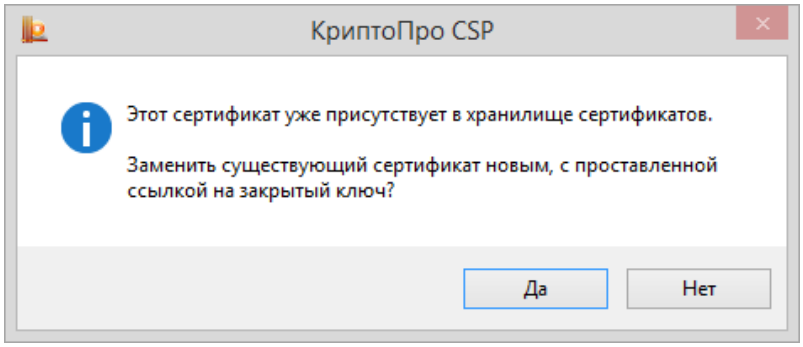


Рисунок 55. Предупреждение о перезаписи сертификата

В случае успеха появится сообщение о завершении операции (см. Рисунок 56).

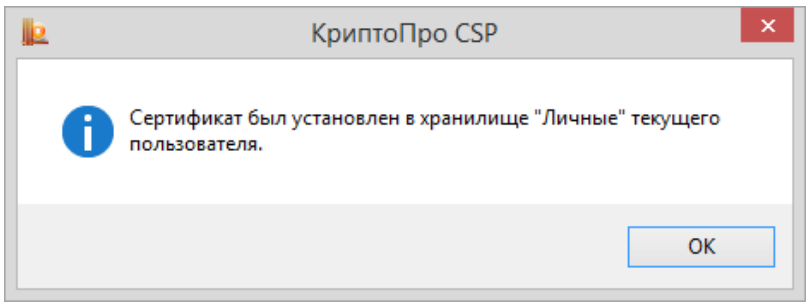


Рисунок 56. Окно завершения установки сертификата

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

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

Для того чтобы установить личный сертификат откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Установить личный сертификат**.

В окне «Расположение файла сертификата» (см. Рисунок 57) будет предложено указать **Имя файла сертификата**. Выберите путь к файлу с помощью кнопки Обзор, после чего нажмите кнопку **Далее.**

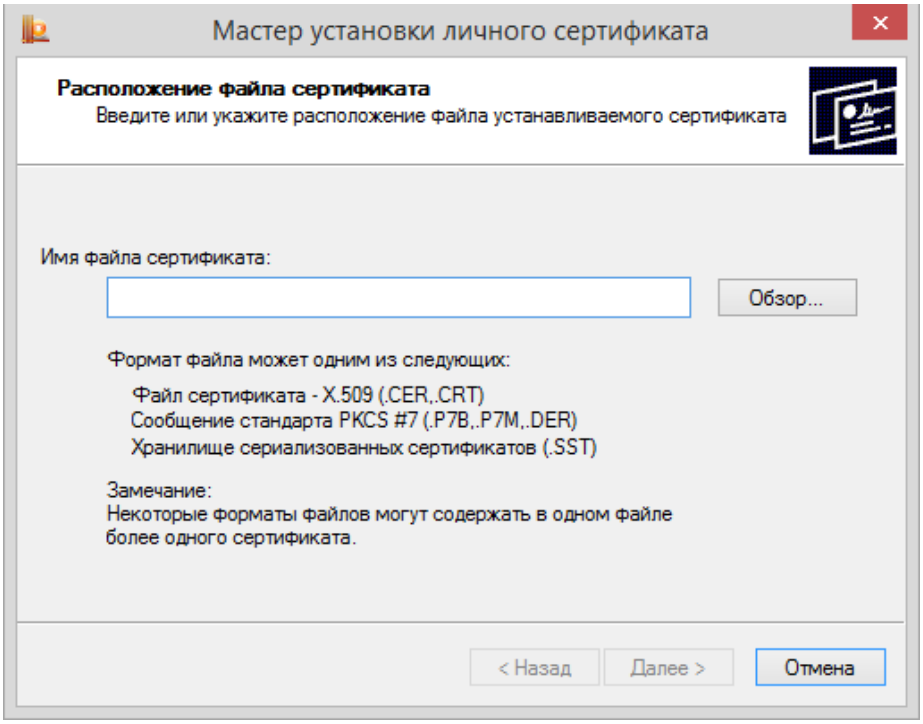


Рисунок 57. Окно «Расположение файла сертификата»

Откроется просмотр основной информации сертификата для установки (см. Рисунок 58). Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

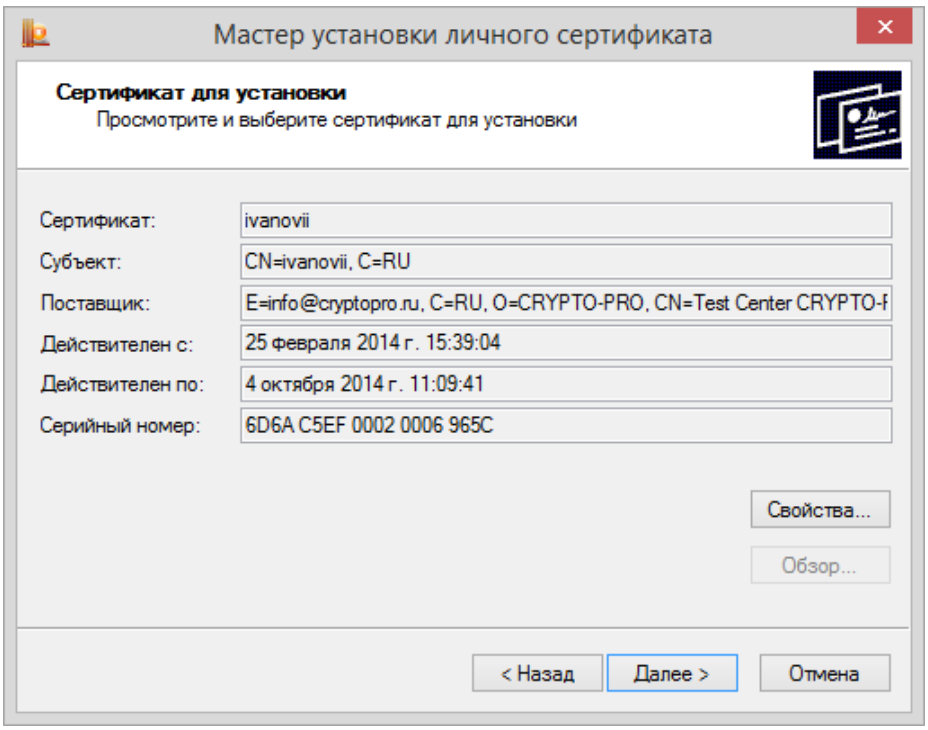


Рисунок 58. Окно «Сертификат для установки»

Нажмите кнопку Далее. Откроется окно «Контейнер закрытого ключа» (см. Рисунок 59).

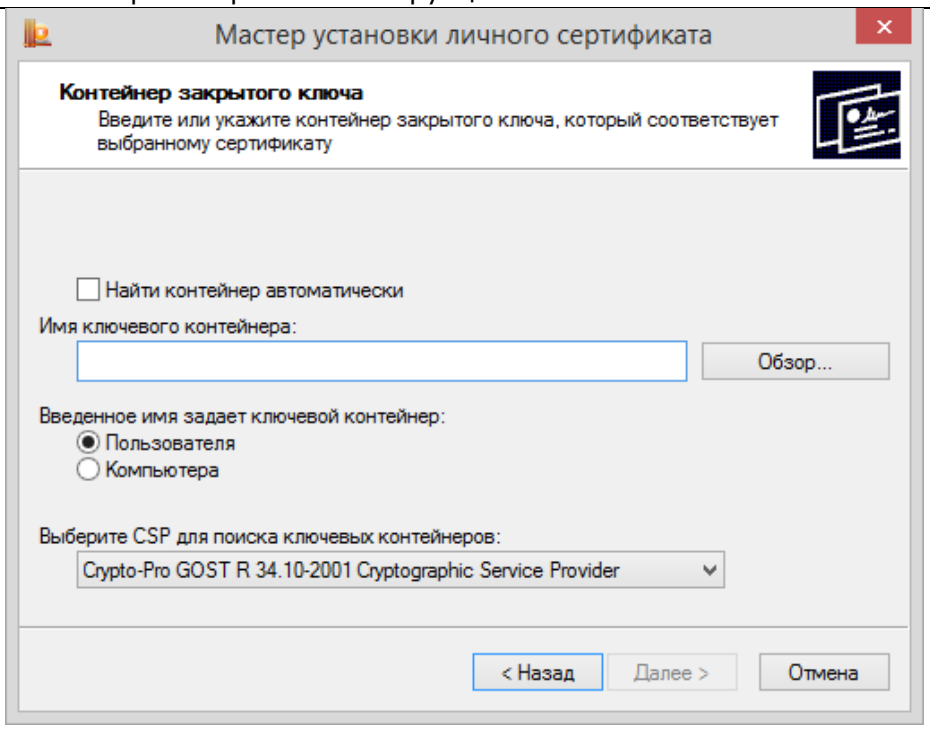


Рисунок 59. Окно «Контейнер закрытого ключа»

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

Опции поиска:

- **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 того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то он будет запрошен. Введите пароль и нажмите кнопку **ОК**.

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

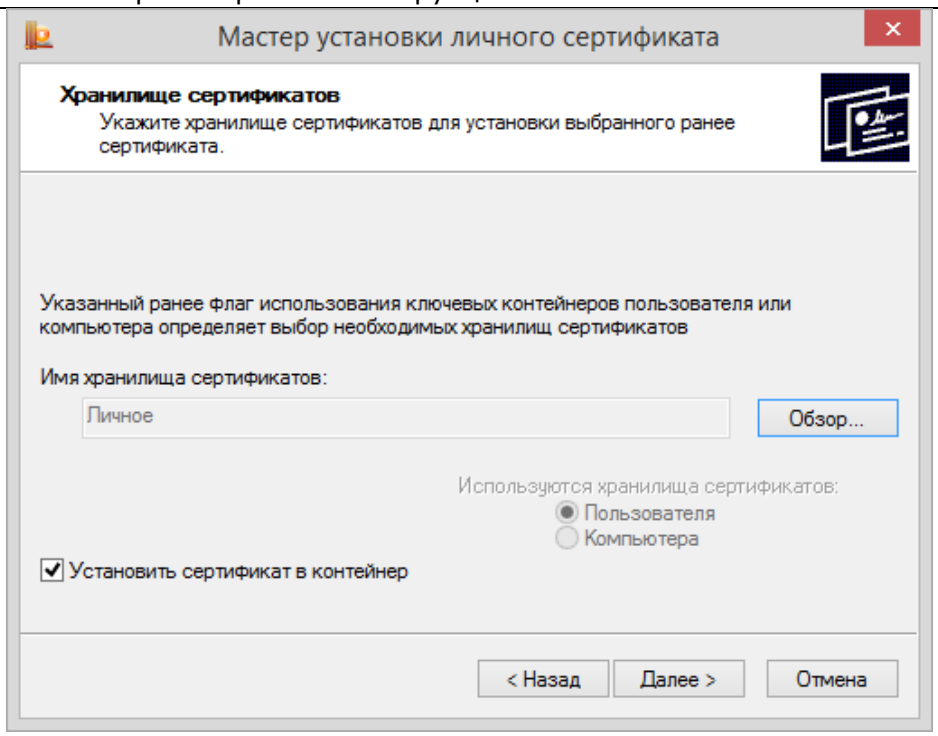


Рисунок 60. Окно «Хранилище сертификатов»

Одновременно сертификат можно записать в ключевой контейнер для удобства поиска сертификата при переносе контейнера на другой компьютер. Для этого служит опция «Установить сертификат в контейнер» (см. Рисунок 60).

На последнем шаге «Завершение работы мастера установки личного сертификата» (см. Рисунок 61) нужно проверить правильность указанных параметров и для выполнения установки сертификата нажать кнопку **Готово**.

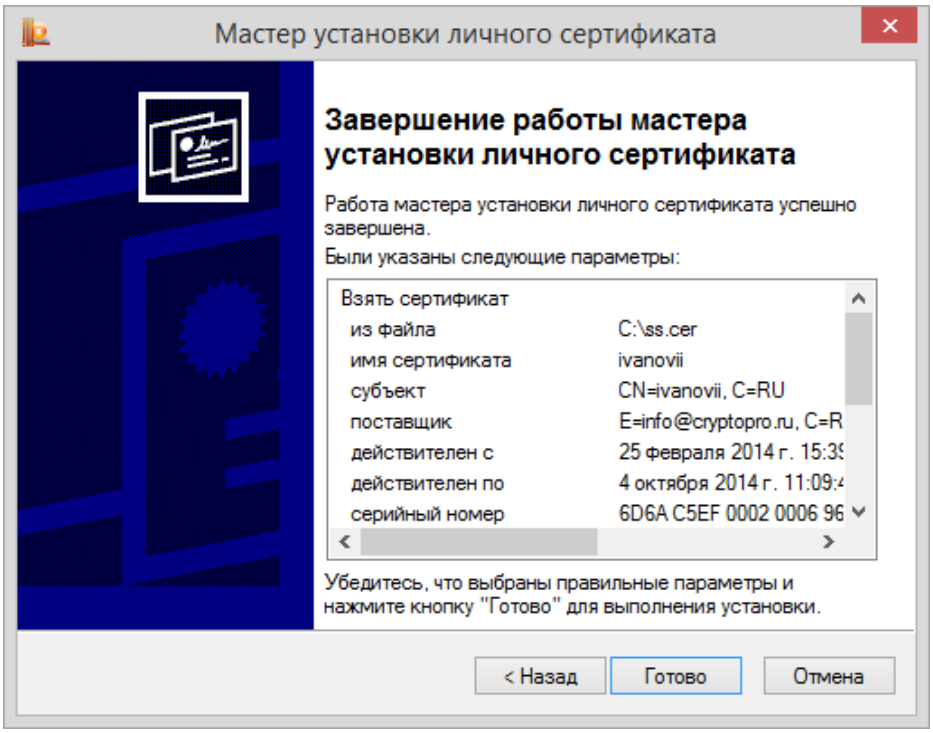


Рисунок 61. Завершение работы мастера установки личного сертификата

2.5.4. Управление паролями доступа к закрытым ключам

2.5.4.1. Изменение пароля на доступ к закрытому ключу

Для того, чтобы изменить пароль на контейнер, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Изменить пароль**.

Откроется окно «Контейнер закрытого ключа» (см. Рисунок 62).

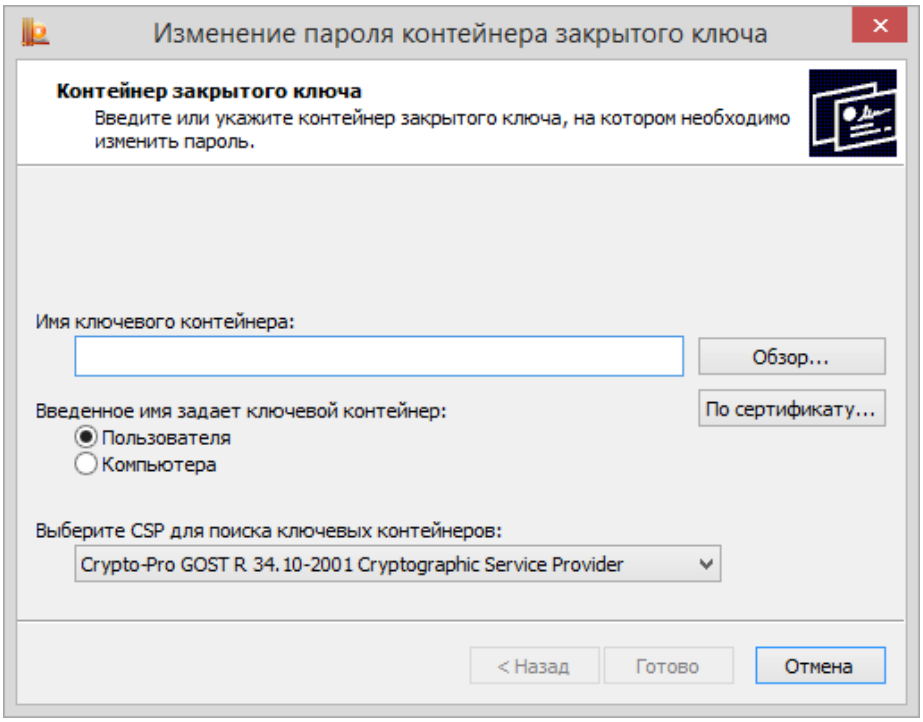


Рисунок 62. Окно «Контейнер закрытого ключа»

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

Опции поиска:

- **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. 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 того, как все поля заполнены, нажмите кнопку **Готово**.

Откроется окно ввода пароля на доступ к закрытому ключу выбранного контейнера (см. Рисунок 63). Введите указанный пароль и нажмите кнопку **ОК.**

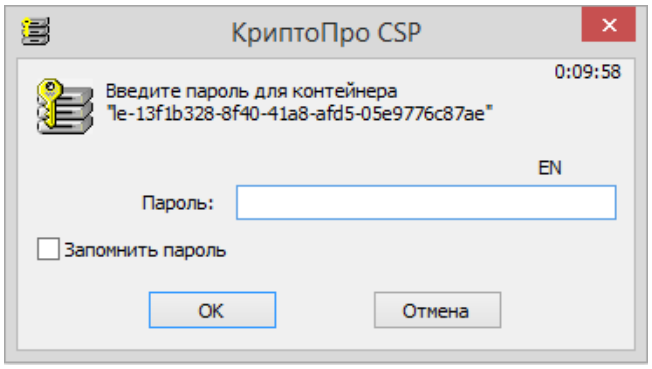


Рисунок 63. Ввод пароля на доступ

Если пароль введен верно, откроется окно ввода нового пароля на доступ к закрытому ключу (см. Рисунок 64). Введите дважды новый пароль и нажмите кнопку **ОК.**

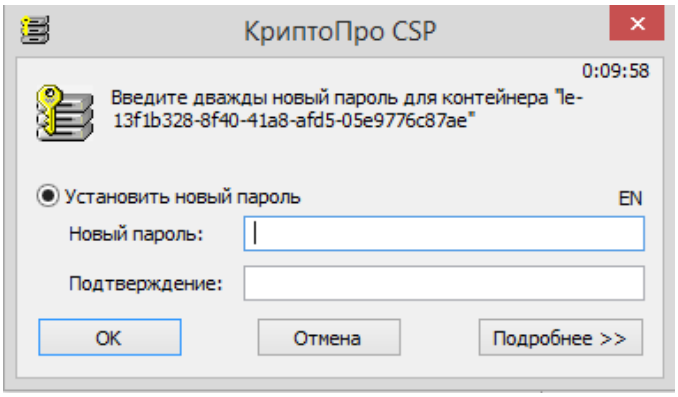


Рисунок 64. Ввод нового пароля

После подтверждения ввода пароля СКЗИ «КриптоПро CSP» осуществит смену пароля 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 разделе 3.2.4.

2.5.4.2. Удаление запомненных паролей

СКЗИ «КриптоПро CSP» позволяет сохранить в специальном хранилище локального компьютера пароли на доступ к контейнеру закрытого ключа (в случае, если пользователь ставит флаг **Запомнить пароль** в окне ввода пароля на доступ к закрытому ключу). 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 того, чтобы удалить запомненный пароль, откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Сервис** (см. Рисунок 40), нажмите кнопку **Удалить запомненные пароли.**

Откроется окно «Удаление запомненных паролей» (см. Рисунок 65).

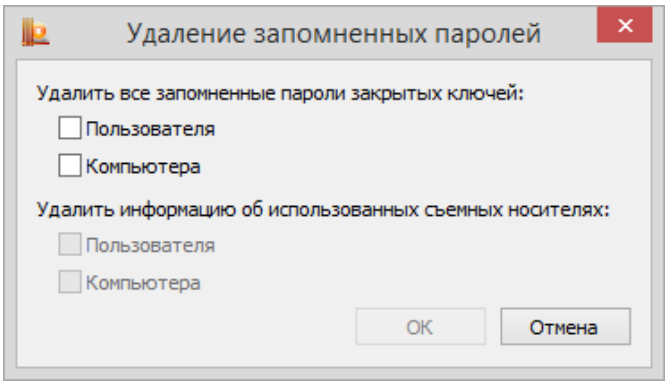


Рисунок 65. Окно «Удаление запомненных паролей»

В этом окне установите флаги **Пользователя/Компьютера** для удаления сохраненных на локальном компьютере в специальном хранилище паролей и нажмите кнопку **ОК**. 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 со СКЗИ «КриптоПро CSP».

Для того, чтобы установить параметры 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 11). После перезапуска перейдите на вкладку **Безопасность** (см. Рисунок 66).

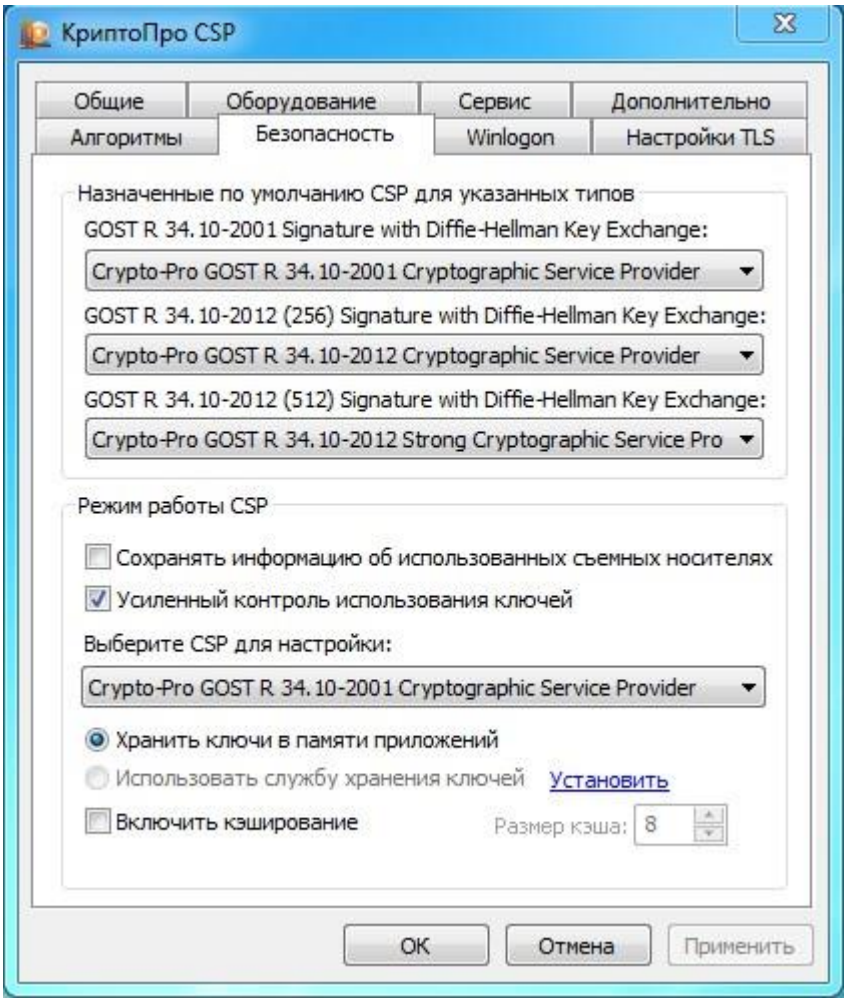


Рисунок 66. Контрольная панель. Вкладка «Безопасность»

На вкладке Безопасность можно выбрать режим работы: с хранением ключей в памяти приложений либо 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. В исполнениях СКЗИ, сертифицированных по уровню КС2 или КС3, режим работы с хранением ключей в службе является единственным доступным (см. Рисунок 67).

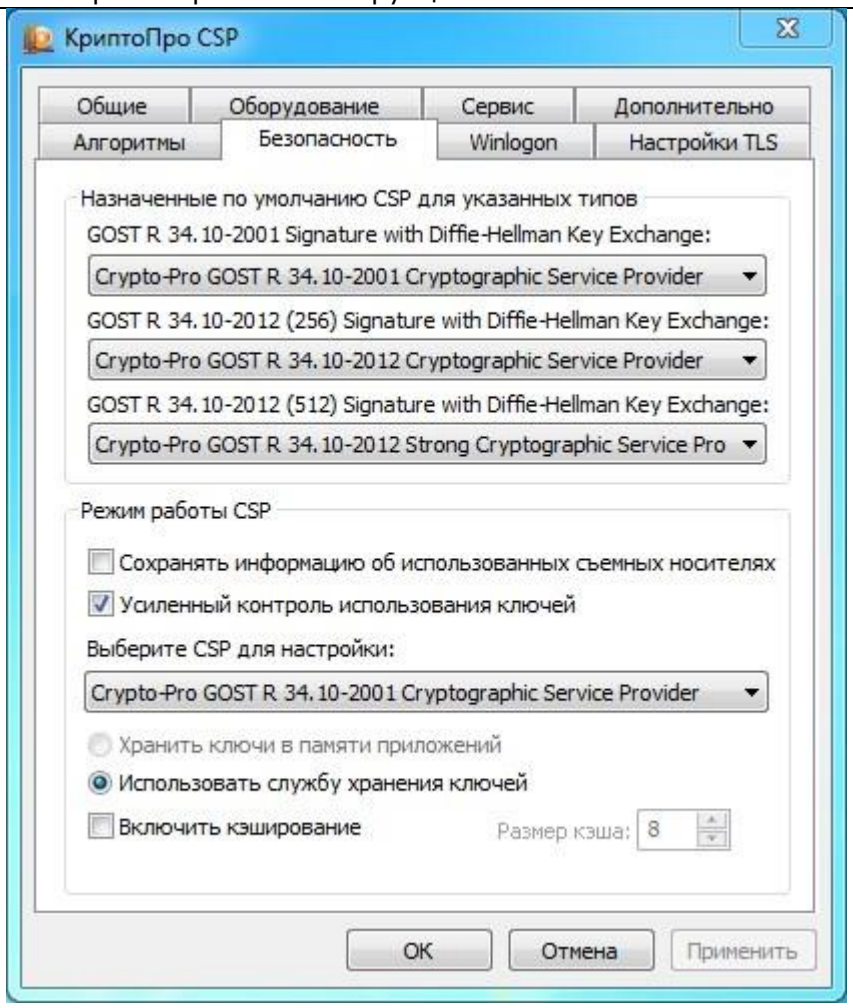


Рисунок 67. Вкладка Безопасность, уровень защиты КС2 или КС3

При хранении ключей в службе хранения ключей возможно применение кэширования контейнеров закрытых ключей. Кэширование заключается в том, что считанные с носителя ключи остаются в памяти сервиса.

Ключ из кэша является доступным и после извлечения ключевого носителя из считывателя, а также после завершения работы загрузившего этот ключ приложения. 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.

Размер кэша задает количество ключей, которые одновременно могут храниться в памяти.

Для того чтобы включить кэширование, необходимо установить флаг в поле **Включить кэширование**. Необходимо также задать размер кэша в соответствующем поле ввода.

Примечание. Если на доступ к закрытому ключу установлен пароль, пароль не сохранен на локальном компьютере, 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.

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

1) осуществить запуск утилиты csptest.exe

```
csptest.exe -keyset -verifycontext -hard_rng
```

2) 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 ca.cer
```

3) перезагрузить компьютер.

2.7. Дополнительные настройки

Вкладка **Дополнительно** контрольной панели СКЗИ КриптоПро CSP предназначена для:

- просмотра версий и путей размещения используемых СКЗИ «КриптоПро CSP» файлов;
- 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 68).

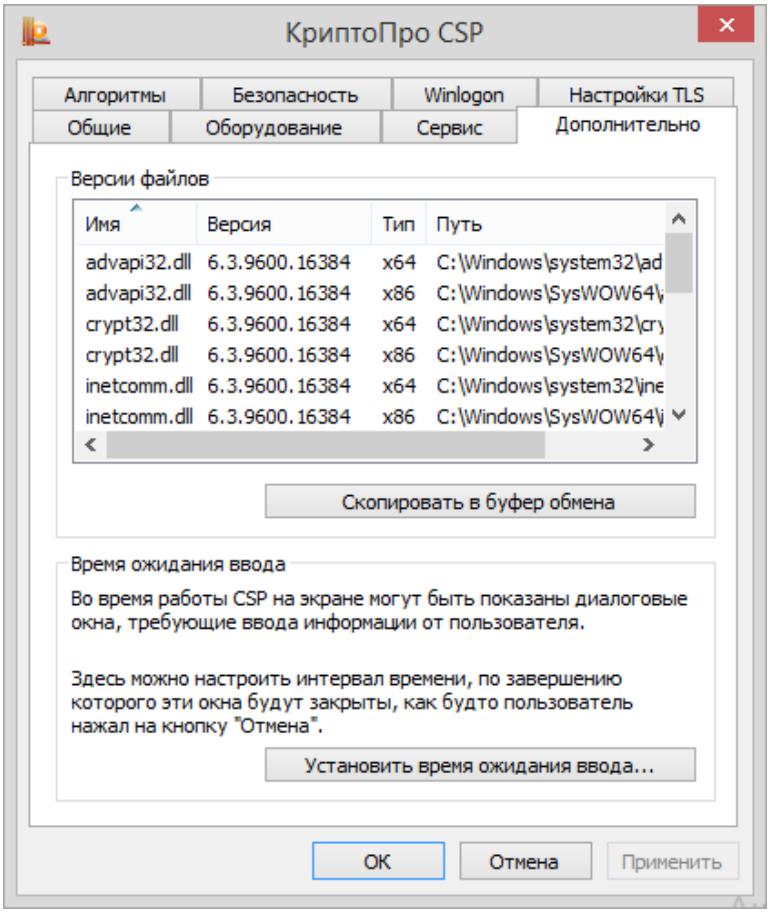


Рисунок 68. Контрольная панель. Вкладка «Дополнительно»

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. 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 68).

Нажмите кнопку **Установить время ожидания ввода.**

Откроется окно «Интервал времени ожидания ввода» (см. Рисунок 69). Установите необходимые значения переключателей **Значение пользователя** и **Значение по умолчанию для всего компьютера**.

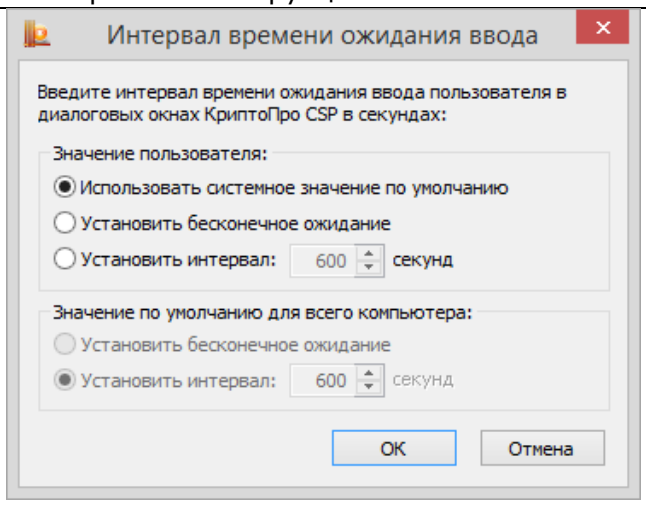


Рисунок 69. Окно «Интервал времени ожидания ввода»

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 40), 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 криптографических алгоритмов.

Для установки параметров криптографических алгоритмов откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Алгоритмы** (см. Рисунок 70):

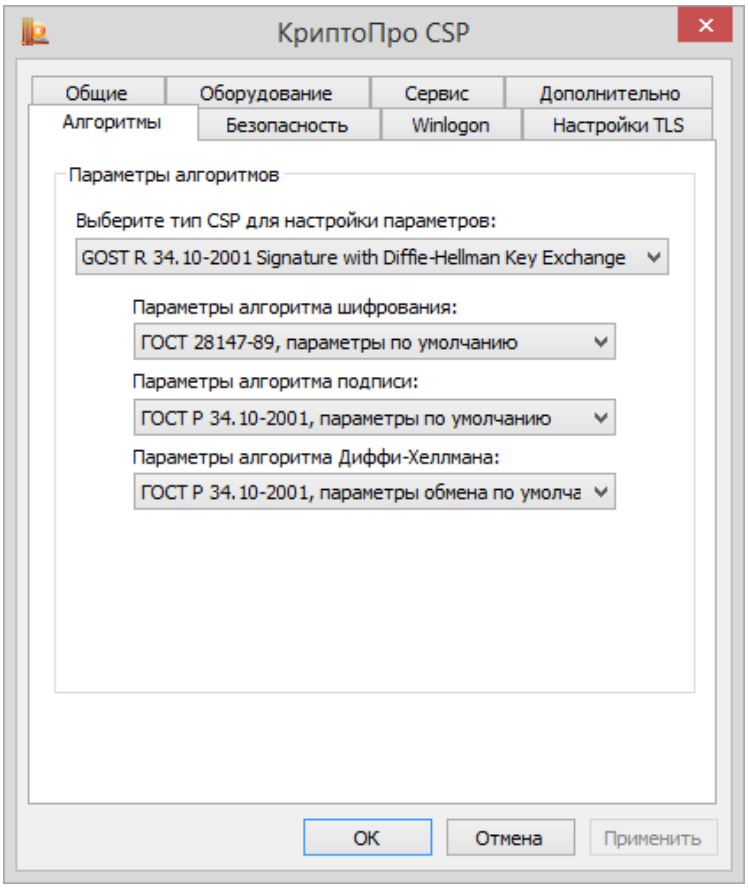


Рисунок 70. Контрольная панель. Вкладка «Алгоритмы»

На закладке **Алгоритмы** можно выбрать тип криптопровайдера, для которого будет осуществляться настройка (в версии КриптоПро CSP 3.6 доступен единственный тип криптопровайдера: GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange), после чего для соответствующих криптографических алгоритмов реализована возможность установки параметров:

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

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 настройки Winlogon откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Winlogon** (см. Рисунок 71):

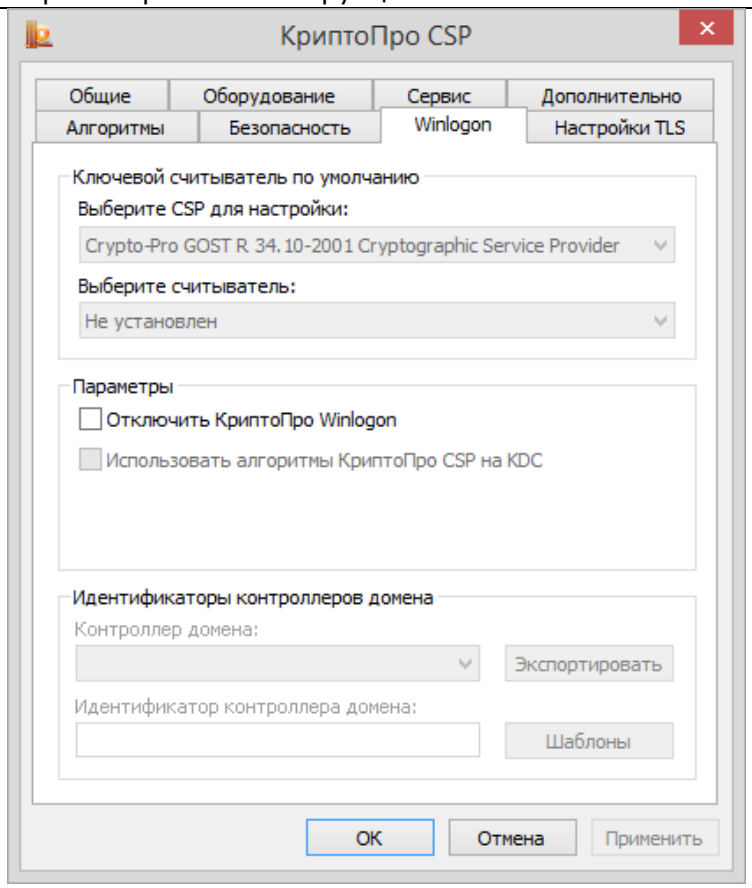


Рисунок 71. Контрольная панель, вкладка Winlogon

При установке на контроллер домена будет доступна для выбора опция **Использовать алгоритмы КриптоПро CSP на KDC** и будут заполнены поля идентификаторов контроллера домена. Подробно о настройке Winlogon см. соответствующую документацию.

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

2.10. Настройки TLS.

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

Для настройки TLS откройте Панель управления СКЗИ КриптоПро CSP и перейдите на вкладку **Настройка TLS** (см. Рисунок 72).

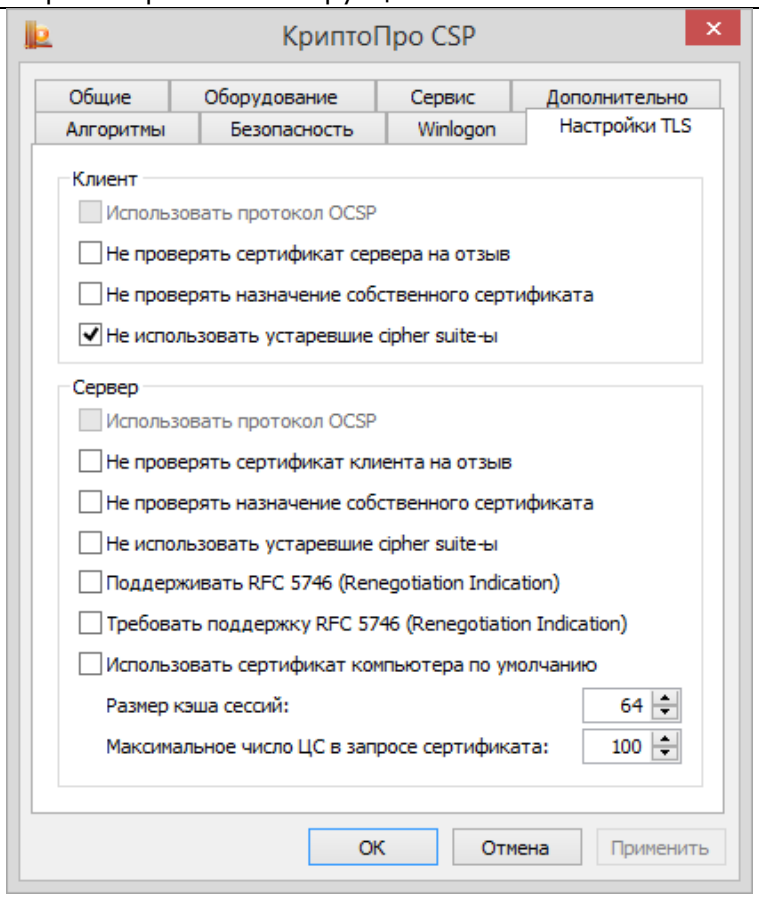


Рисунок 72. Контрольная панель, вкладка Настройка TLS

В параметрах клиента:

флаг **Использовать протокол OCSP** – клиентом осуществляется протокол проверки сертификата по базе сервера OCSP Responder;

флаг **Не проверять сертификат сервера на отзыв** – клиентом не производится проверка сертификатов на принадлежность списку отозванных сертификатов (CRL);

флаг **Не проверять назначение собственного сертификата** –

флаг **Не использовать устаревшие cipher suite-ы** – отключается возможность использования cipher suite, в которых были обнаружены уязвимости.

Необходимо требовать поддержку RFC 5746.

В параметрах сервера:

флаг **Использовать протокол OCSP** – сервером осуществляется протокол проверки сертификата по базе сервера OCSP Responder.

Путем установления соответствующих флагов в полях сервера достигается отключение сервером проверки сертификата клиента на наличие в списке отозванных сертификатов, проверки назначения собственного сертификата, использование cipher suite, в которых были обнаружены уязвимости.

Посредством установления/снятия флагов, связанных с расширением Renegotiation Indication, контролируется требование безопасного связывания нескольких фаз handshake (см. RFC 5746).

В соответствующих полях настраивается размер кэша сессий и максимальное число центров сертификации в запросе сертификата.

3. Интерфейс генерации ключей

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

Примечание. В операционных системах Windows в случае использования службы хранения ключей для уровня КС1 (см. раздел Установка параметров безопасности) или использования Биологического датчика случайных чисел для уровней КС2/КС3 (см. раздел Настройка датчиков случайных чисел) диалоги выбора считывателя и генерации ключа появляются на сервисном десктопе.

3.1. Генерация ключей и получение сертификата при помощи УЦ

Для формирования личных ключей и получения сертификатов можно воспользоваться тестовым Центром Сертификации https://www.cryptopro.ru/certsrv.

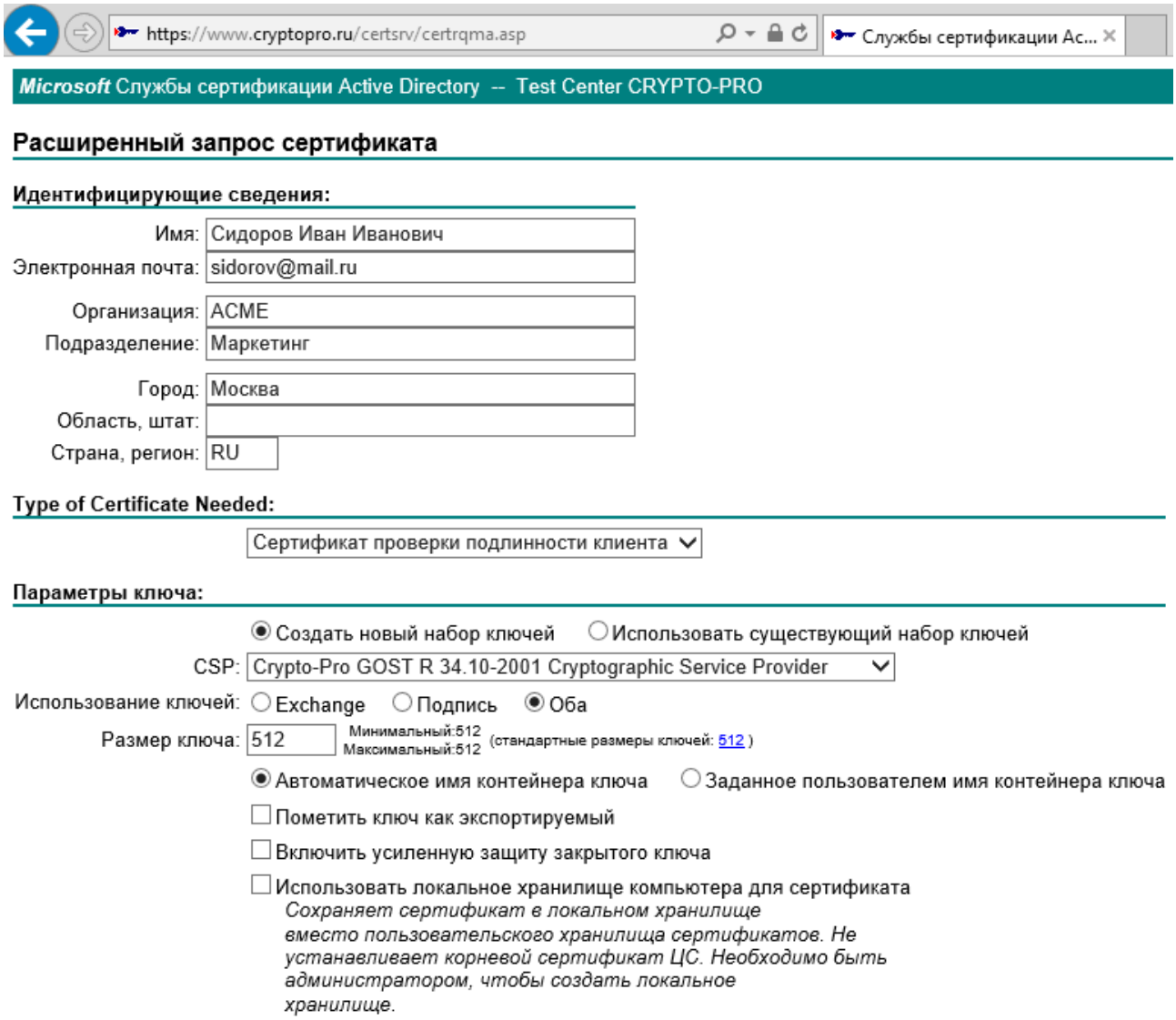


Рисунок 73. Генерация ключа при помощи УЦ

В диалоге создания ключа и формирования запроса на сертификат задайте "Имя Владельца" сертификата и введите свой адрес электронной почты "Адрес E-Mail".

Если запрашиваемый сертификат предполагается использовать в электронной почте, выберите Сертификат защиты электронной почты **Область применения ключа**.

Если запрашиваемый сертификат предполагается использовать в протоколе TLS, выберите **Сертификат аутентификации клиента** в разделе **Область применения ключа**.

Примечание. Если введенный адрес почты не совпадает с зарегистрированным адресом в

Outlook Express (Outlook), использовать криптографические функции в электронной почте будет невозможно.

3.2. Создание ключевого контейнера

3.2.1. Выбор ключевого носителя

При создании ключевого контейнера откроется окно выбора ключевого носителя (см. Рисунок 74).

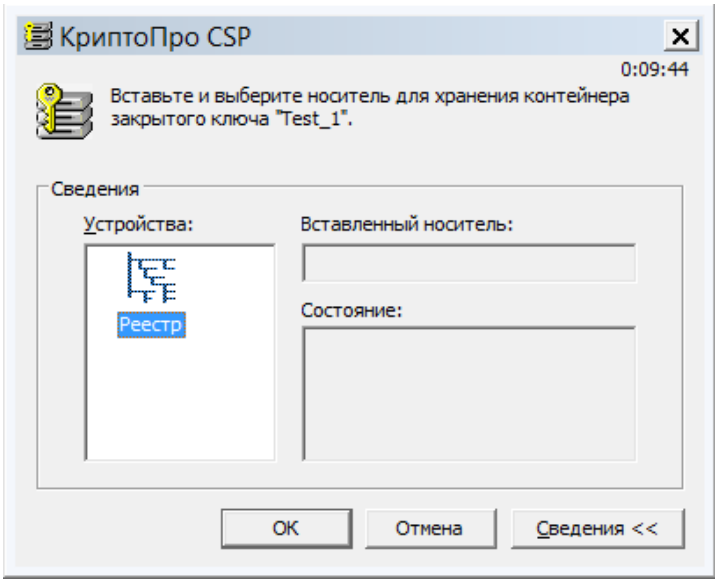


Рисунок 74. Выбор ключевого носителя

Это окно отображается в том случае, когда пользователь имеет несколько устройств, служащих ключевыми считывателями. В случае, когда ключевой считыватель только один, он выбирается автоматически, и это окно не отображается.

После того, как ключевой считыватель выбран, нажмите кнопку **ОК**.

3.2.2. Генерация начальной последовательности ДСЧ

После выбора ключевого считывателя, если в системе не установлен аппаратный ДСЧ, откроется окно «Биологический датчик случайных чисел» (см. Рисунок 75).

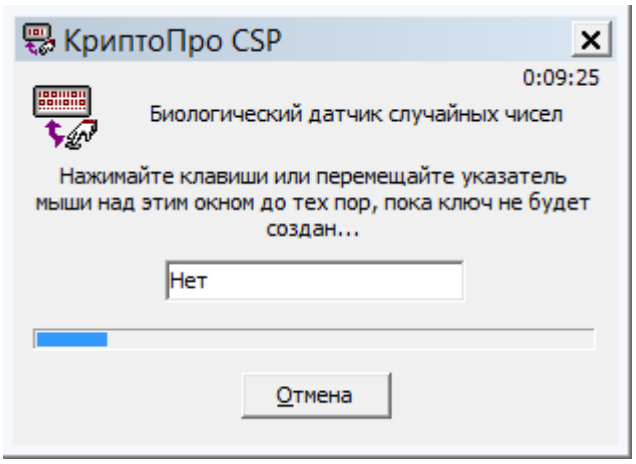


Рисунок 75. Биологический датчик случайных чисел

Биологический датчик случайных чисел предназначен для генерации начальной последовательности датчика случайных чисел.

Для генерации необходимо нажимать на клавиши или двигать мышью.

3.2.3. Ввод пароля на доступ к закрытому ключу

После завершения работы биологического датчика случайных чисел откроется окно ввода пароля на доступ к закрытому ключу создаваемого контейнера (см. Рисунок 76).

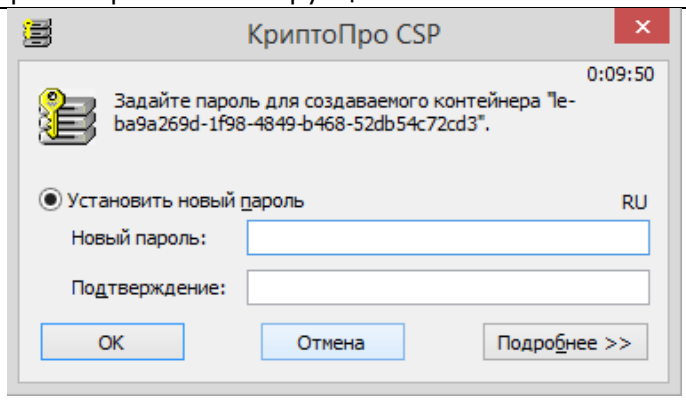


Рисунок 76. Ввод пароля на доступ к закрытому ключу

В поле **Новый пароль** пользователь должен ввести текстовый пароль на доступ к закрытому ключу создаваемого контейнера и подтвердить его повторным вводом в поле **Подтверждение**.

После ввода пароля нажмите кнопку **ОК**.

Если ключ генерируется на носитель, поддерживающий аппаратный пароль или пин-код, то необходимо ввести тот пароль (пин-код), который установлен на этот ключевой носитель.

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 в окне ввода пароля на доступ к закрытому ключу создаваемого контейнер (см. Рисунок 76) нажмите кнопку **Подробнее**. Откроется окно выбора способа защиты доступа к закрытому ключу создаваемого контейнера (см. Рисунок 77). Защита носителей, поддерживающих аппаратный пароль (пин-код), возможна только на этом пароле (пин-коде).

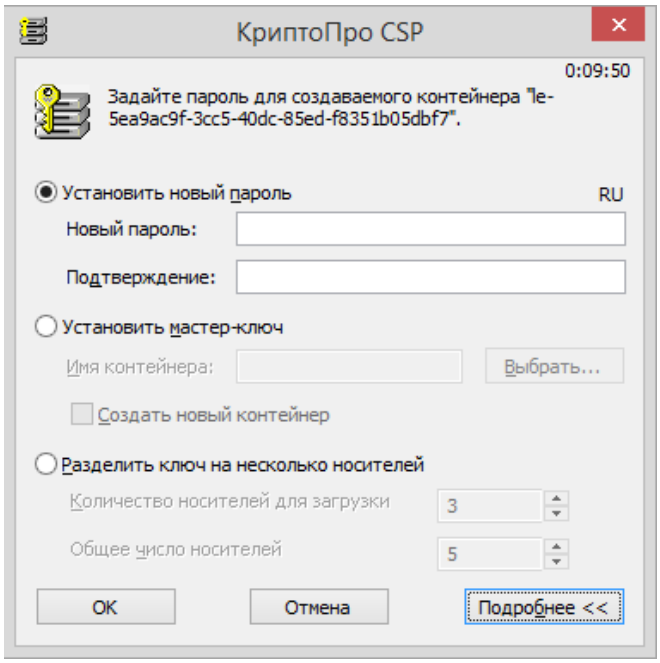


Рисунок 77. Выбор средства защиты доступа к закрытому ключу

В этом окне содержатся следующие поля:

- **Установить новый пароль** – ввод текстового пароля;
- **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 на поле **Установить новый пароль** (см. Рисунок 77), то СКЗИ КриптоПро CSP осуществит защиту ключа при помощи пароля на доступ, введенного с клавиатуры. Необходимо осуществить действия, описанные в пункте Ввод пароля на доступ к закрытому ключу.

3.2.4.2. Установка мастер-ключа

Если переключатель на поле **Установить мастер-ключ** (см. Рисунок 77), 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 78).

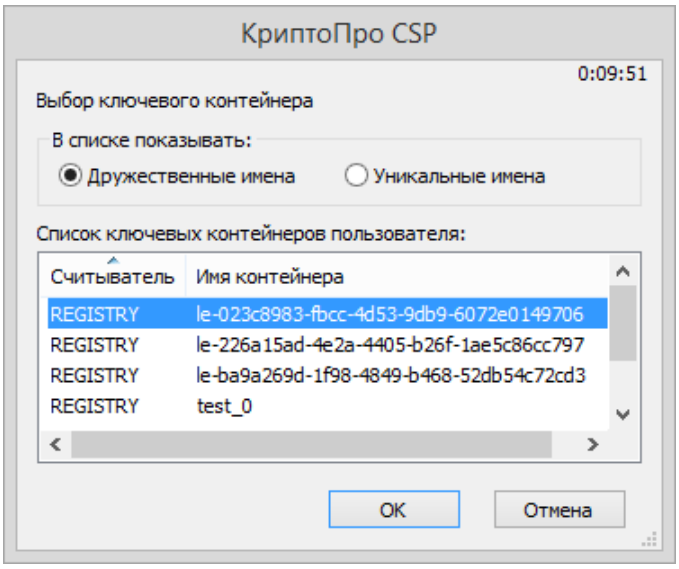


Рисунок 78. Список существующих контейнеров

После выбора необходимого контейнера нажмите кнопку **ОК**. 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 77) аналогично 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 77), 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.

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 74). В этом окне выберите носитель, который будет участвовать в разделении ключа.
2. После того, как для всех контейнеров выбраны носители, откроется окно ДСЧ.
3. После завершения генерации откроется окно ввода пароля на доступ к закрытому ключу для каждого создаваемого контейнера (см. Рисунок 76). В этом окне нужно ввести или выбрать другое средство защиты доступа к закрытому ключу при помощи кнопки **Подробнее** (см. Рисунок 77).

После создания всех контейнеров, участвующих в разделении ключа, будет обеспечена защита доступа к закрытому ключу.

3.3. Открытие ключевого контейнера

3.3.1. Отсутствие ключевого носителя

В случае отсутствия ключевого носителя при открытии ключевого контейнера появится окно, сообщающее об отсутствии носителя (см. Рисунок 79).

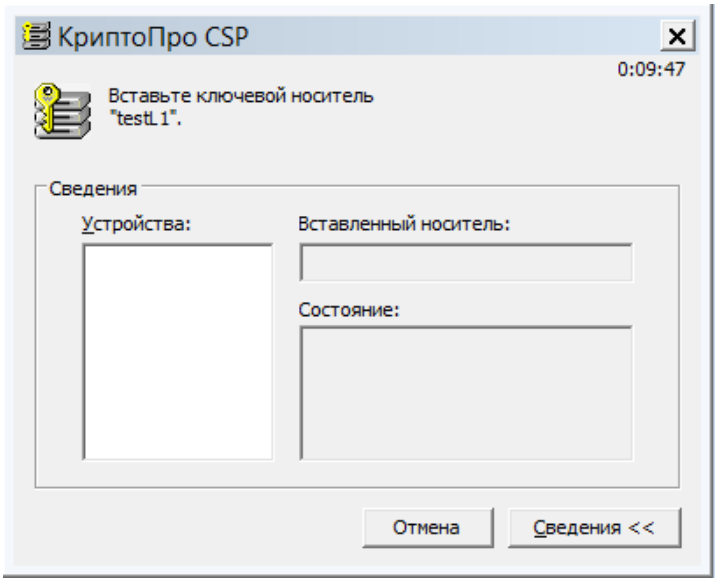


Рисунок 79. Отсутствие необходимого носителя

После того, как носитель будет подключен, откроется следующее окно.

Если требуемый носитель установить не удается, нажмите кнопку **Отмена**.

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

3.3.2. Проверка пароля на доступ к закрытому ключу

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

3.3.2.1. Проверка текстового пароля

Если устанавливалась защита доступа к закрытому ключу с помощью пароля (см. пункт 3.2.4.1), то будет отображено окно проверки пароля для доступа к закрытому ключу открываемого контейнера (см. Рисунок 80).

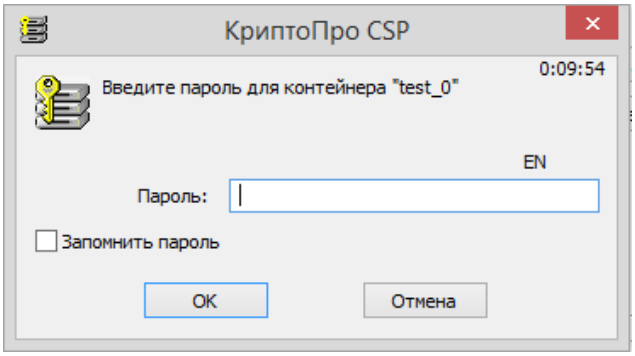


Рисунок 80. Проверка пароля на доступ к закрытому ключу

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.

3.3.2.2. Проверка пароля при зашифровании ключа на другом ключе

Если защита доступа к закрытому ключу была осуществлена 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 80).

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

3.3.2.3. Проверка пароля при разделении ключа между несколькими носителями

Если защита доступа к закрытому ключу осуществлялась 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. При нахождении 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

Для выпуска сертификатов в качестве примера используется Тестовый ЦС на сайте cryptopro.ru

4.1. Установка IIS на сервере.

В случае, если службы IIS не установлены в операционной системе Windows используемой версии по умолчанию, необходимо выполнить установку с помощью пользовательского интерфейса через Компоненты Windows. Для этого через меню Пуск откройте Панель управления, найдите Программы и компоненты, выберите 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:

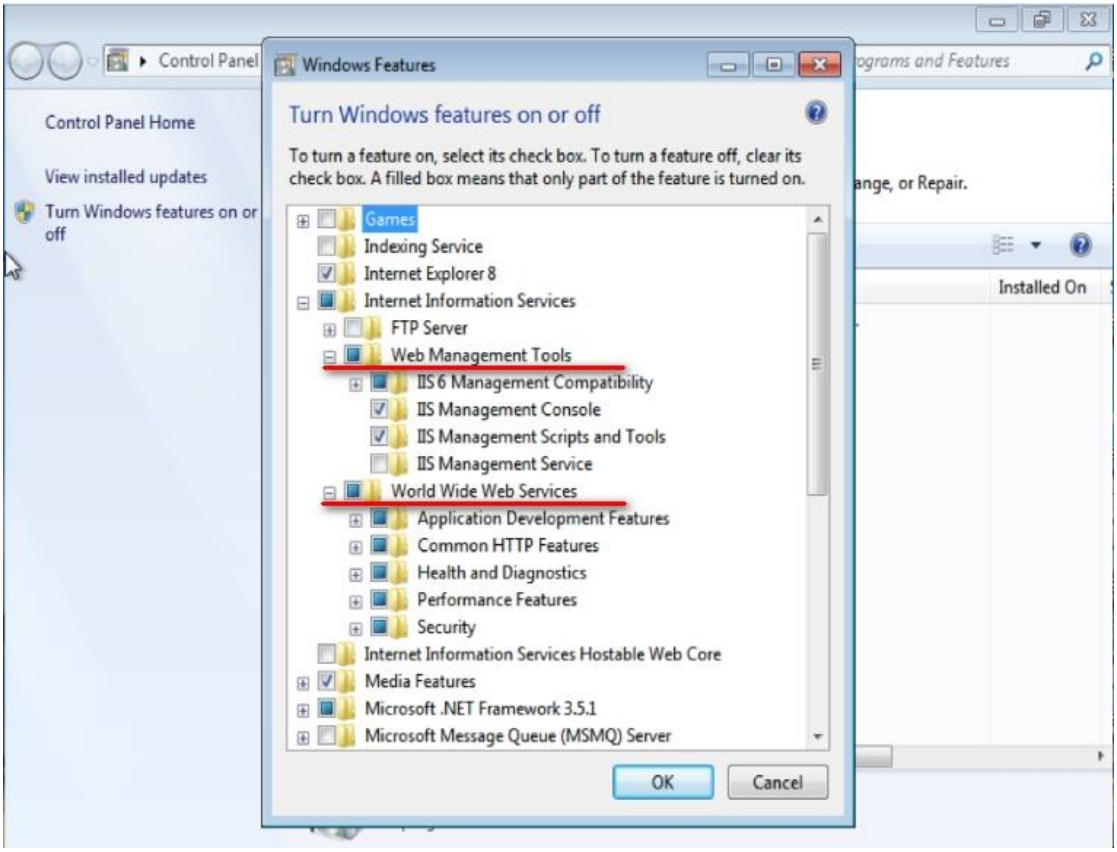


Рисунок 81. Включение компонентов IIS

Нажмите ОК для выполнения настройки сервера.

4.2. Установка КриптоПро CSP

Установка КриптоПро CSP выполняется запуском файла CSPSetup.exe, далее пошагово с помощью мастера установки (см. 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:

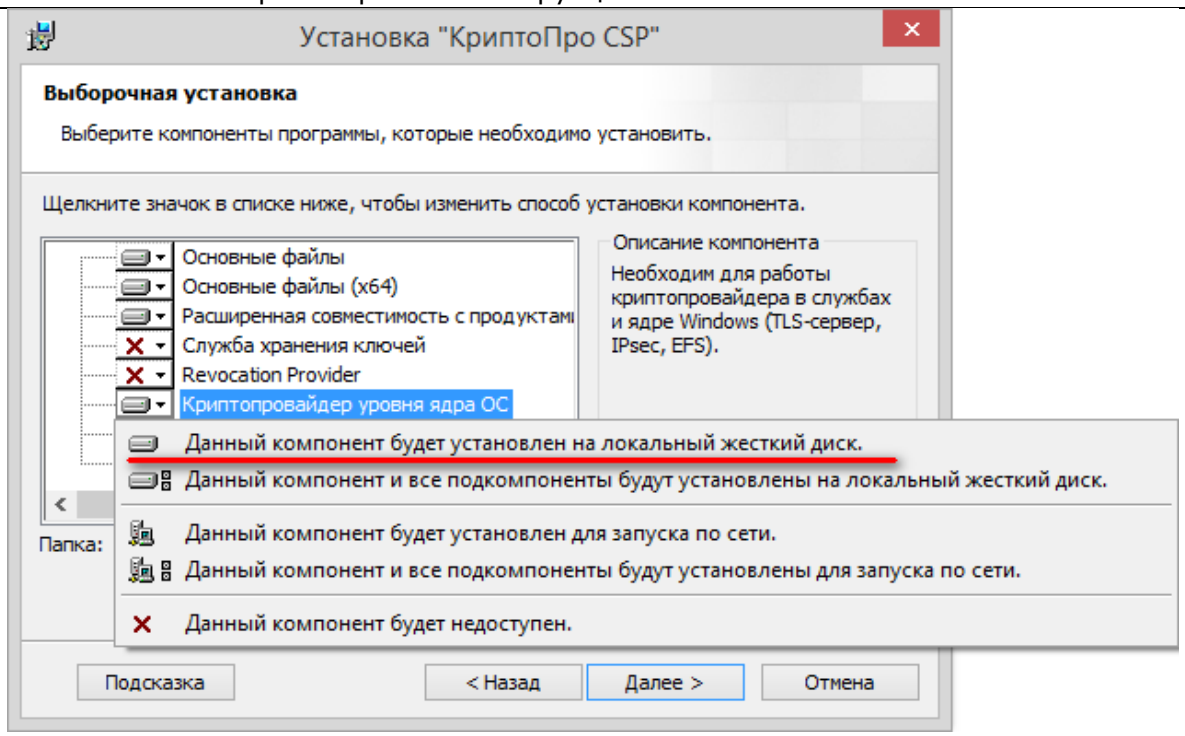


Рисунок 82. Включение компонентов КриптоПро CSP при установке

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 →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 ntcnjdsq центр сертификации 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.

Из списка действий выберите получение сертификата удостоверяющего центра.

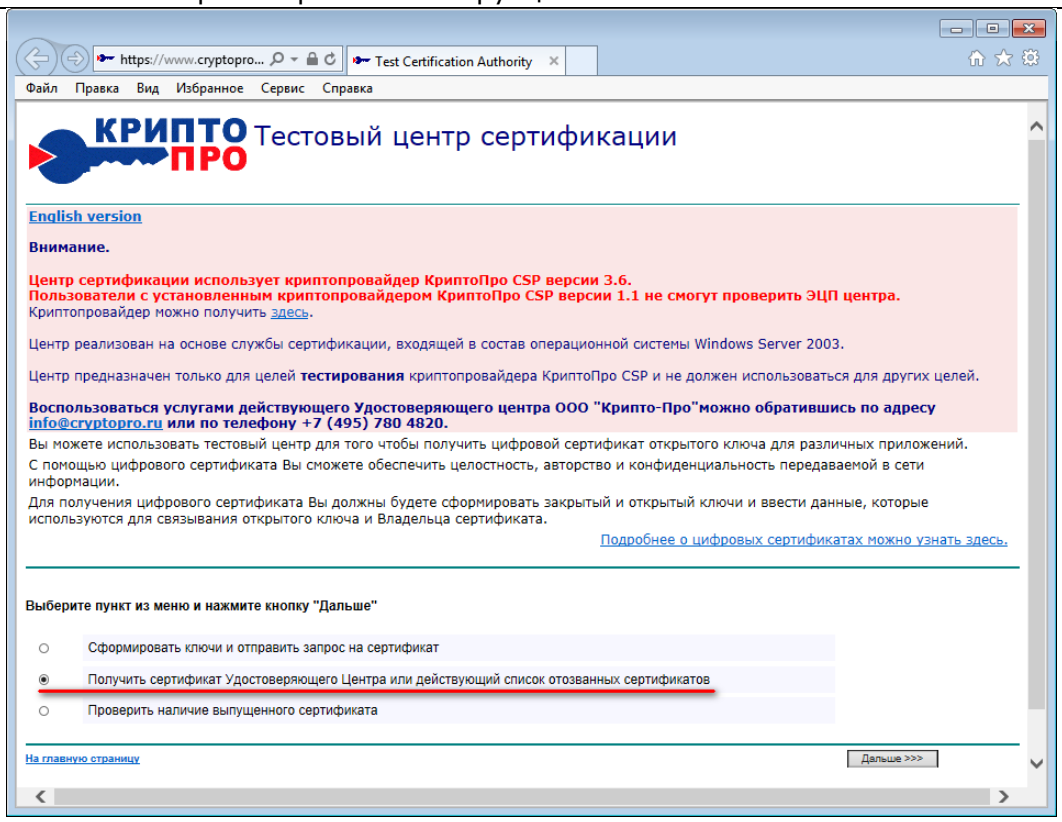


Рисунок 83. Тестовый ЦС

Далее выполняется загрузка сертификата центра сертификации. Выберите метод шифрования и нажмите на ссылку «Загрузка сертификата ЦС».

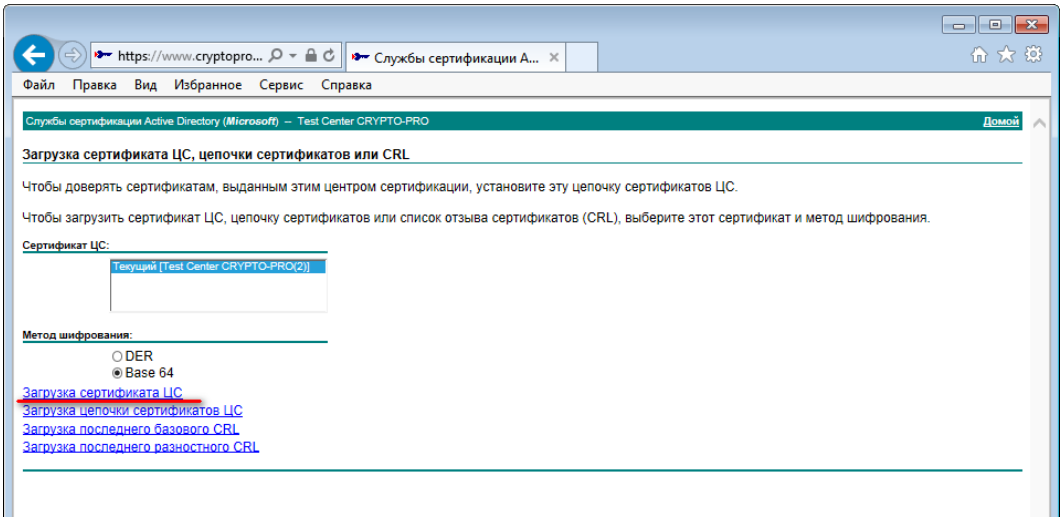


Рисунок 84. Загрузка сертификата ЦС

При получении сертификата нужно выбрать «Открыть сертификат». Если данный сертификат ранее не был установлен в хранилище доверенных корневых центров сертификации, его необходимо установить.

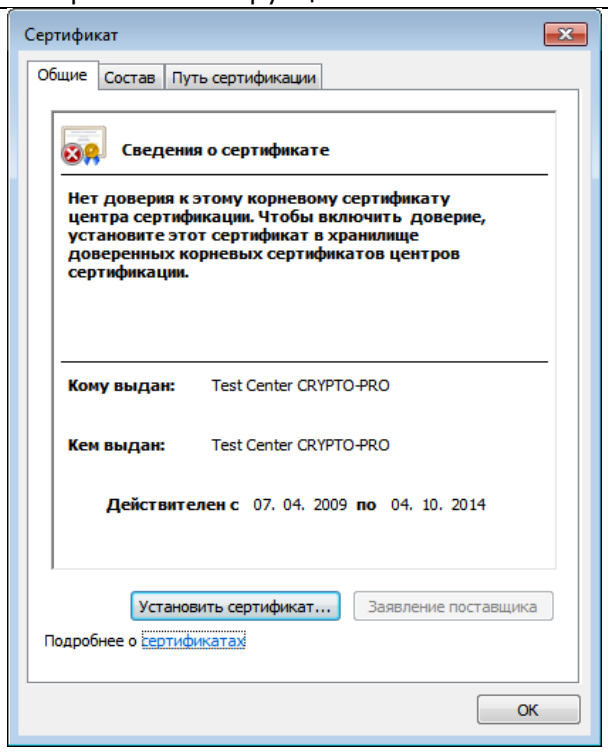


Рисунок 85. Просмотр сертификата ЦС

В окне просмотра сведений о сертификате нажмите кнопку «Установить сертификат», откроется мастер импорта сертификатов.

В диалоге выбора хранилища сертификатов укажите «Поместить сертификаты в следующее хранилище», при выборе хранилища поставьте флажок «Показать физические хранилища», укажите в доверенных корневых центрах сертификации хранилище локального компьютера.

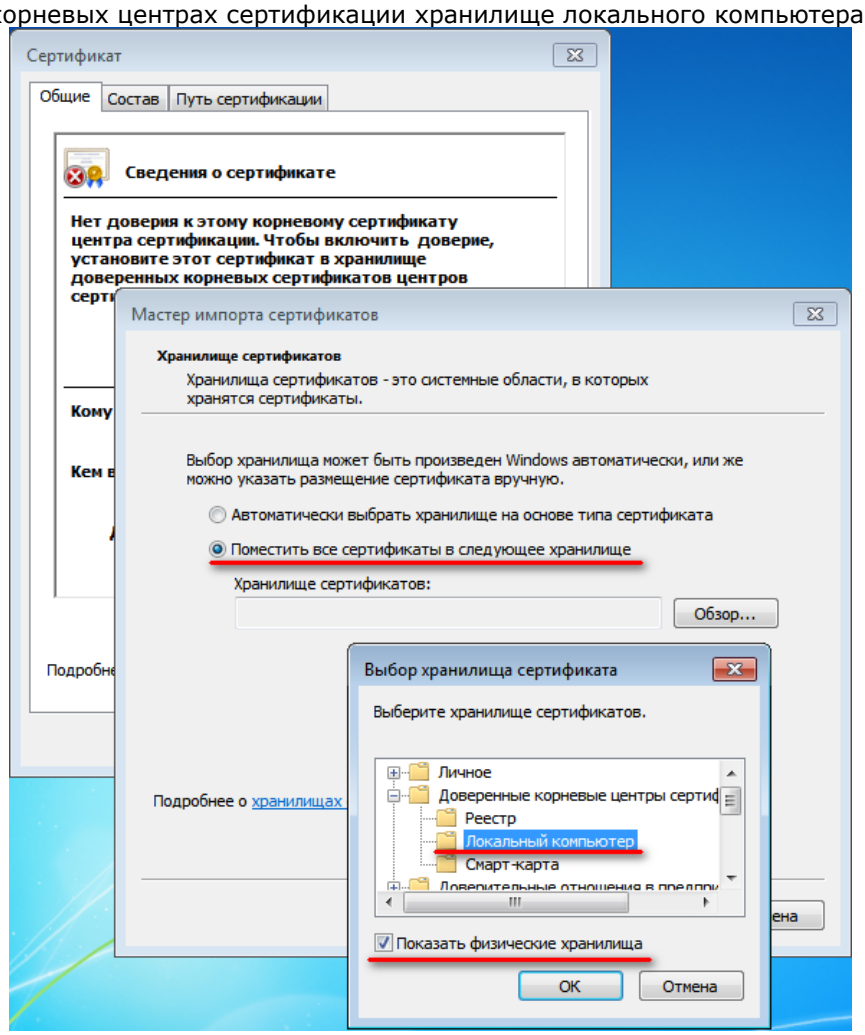


Рисунок 86. Установка сертификата ЦС

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.

Из списка действий выберите получение сертификата удостоверяющего центра (Корневой сертификат необходимо получать доверенным образом).

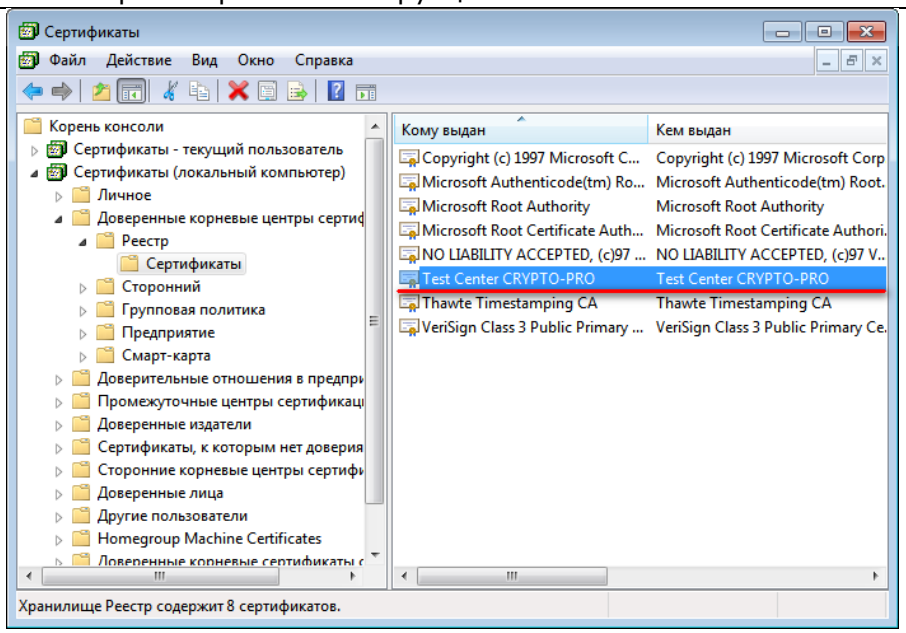


Рисунок 87. Хранилище Доверенные корневые центры сертификации

4.4. Установка сертификата IIS

Для того, чтобы настроить соединение с сервером по протоколу TLS, необходимо предпринять следующие шаги:

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 центр сертификации 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/ и из списка действий выберите «Сформировать ключи и отправить запрос на сертификат».

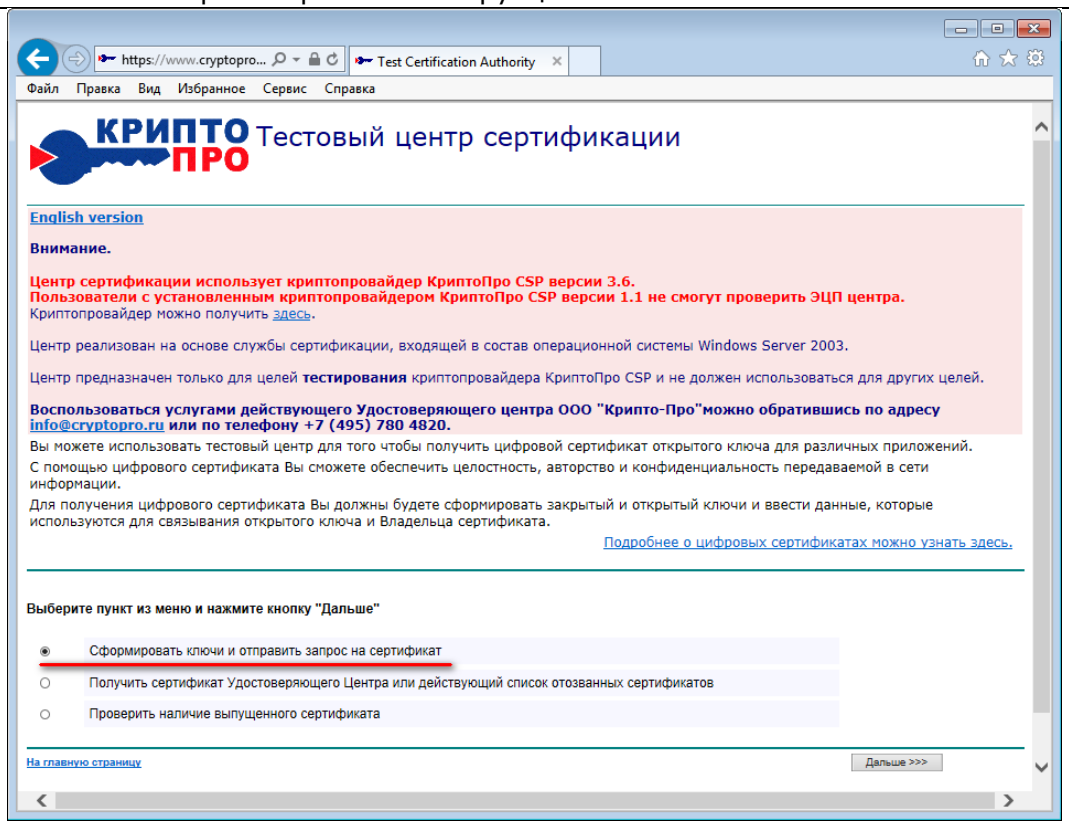


Рисунок 88. Создание ключа и сертификата в тестовом ЦС

На следующем шаге выберите действие «Создать и выдать запрос к этому ЦС».

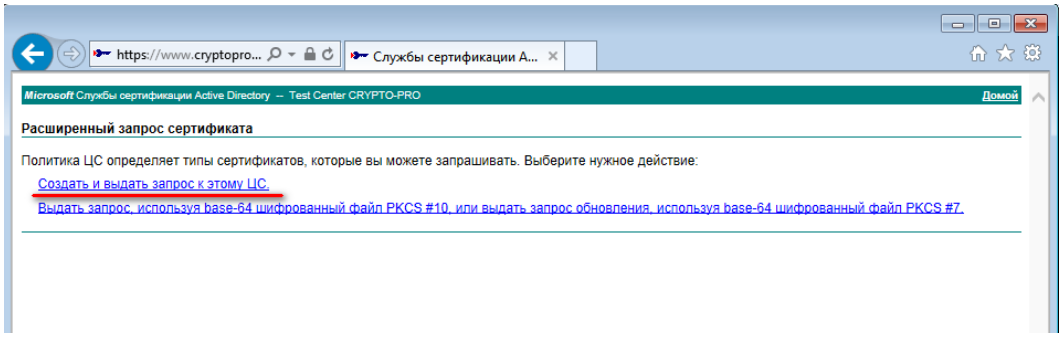


Рисунок 89. Выбор запроса сертификата

В появившемся диалоге подтвердите выполнение операции с сертификатом от имени пользователя.

В открывшейся форме заполните данные сертификата. При заполнении поля Имя (Common Name) необходимо учитывать, что имя сертификата должно совпадать с доменом, обслуживаемым сервером IIS, для которого выпускается сертификат.

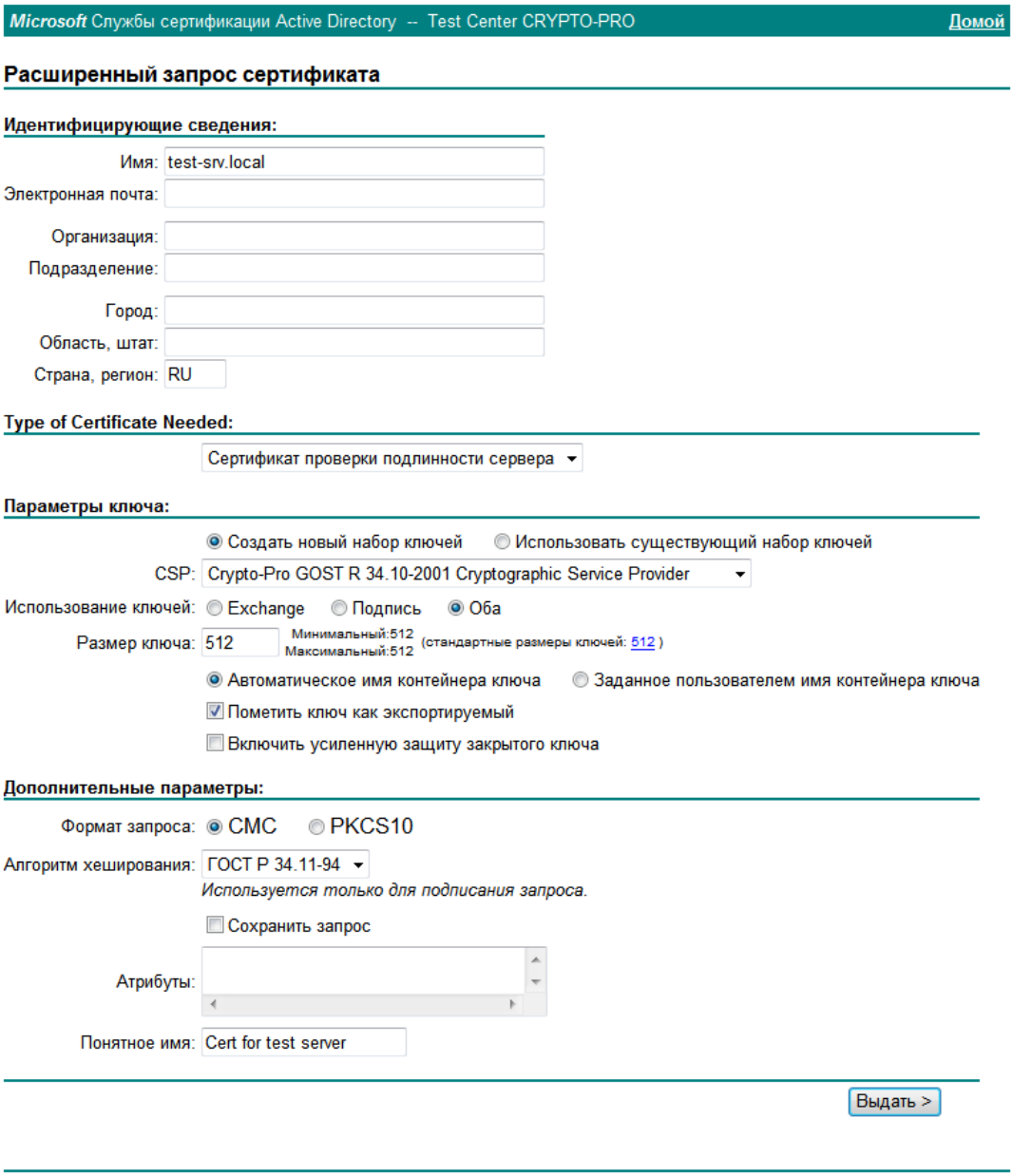


Рисунок 90. Заполнение параметров сертификата IIS в тестовом ЦС

Заполните необходимые поля, укажите тип сертификата «Сертификат проверки подлинности сервера», в параметрах ключа укажите «Использовать новый набор ключей» и выберите CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider. Если в дальнейшем предполагаются манипуляции с ключом сертификата, для удобства можно пометить ключ как экспортируемый и в дополнительных параметрах указать понятное имя. Остальные параметры рекомендуется оставить по умолчанию.

После заполнения полей формы нажмите кнопку «Выдать».

В диалоговом окне будет предложено указать пароль для сертификата. В данном случае пароль не требуется, поля нужно оставить пустыми и нажать кнопку ОК. После завершения работы биологического датчика в браузере открывается страница со ссылкой для установки выпущенного сертификата:

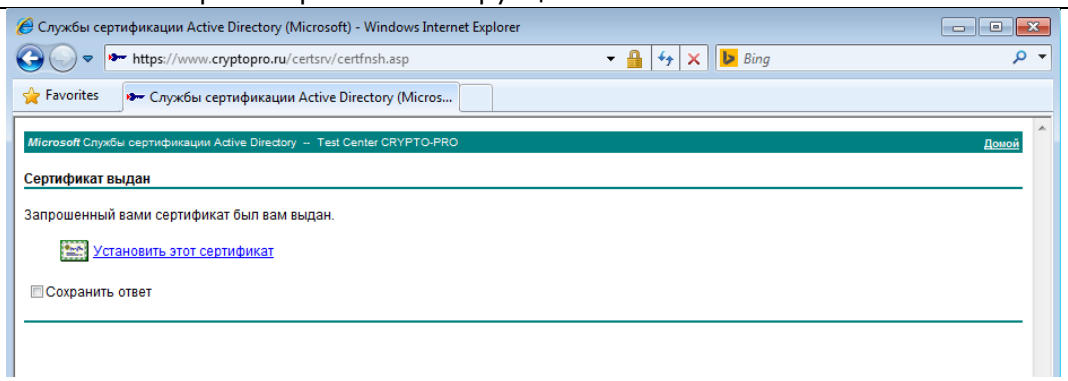


Рисунок 91. Установка созданного через тестовый ЦС сертификата IIS

Нажмите «Установить этот сертификат». На странице появится 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 службы IIS должен находиться в хранилище Личное локального компьютера.

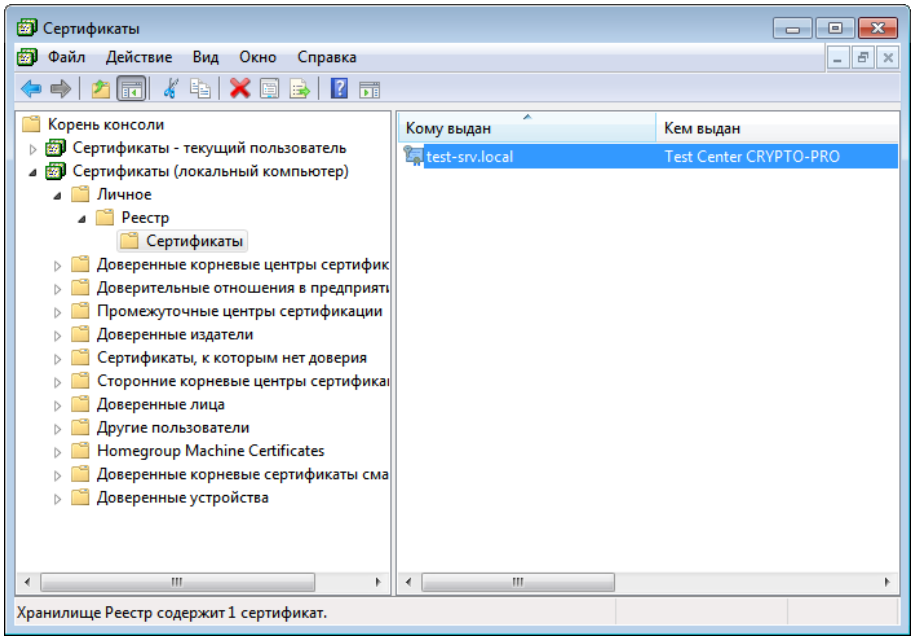


Рисунок 92. Проверка наличия сертификата IIS в хранилище локального компьютера

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

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…)

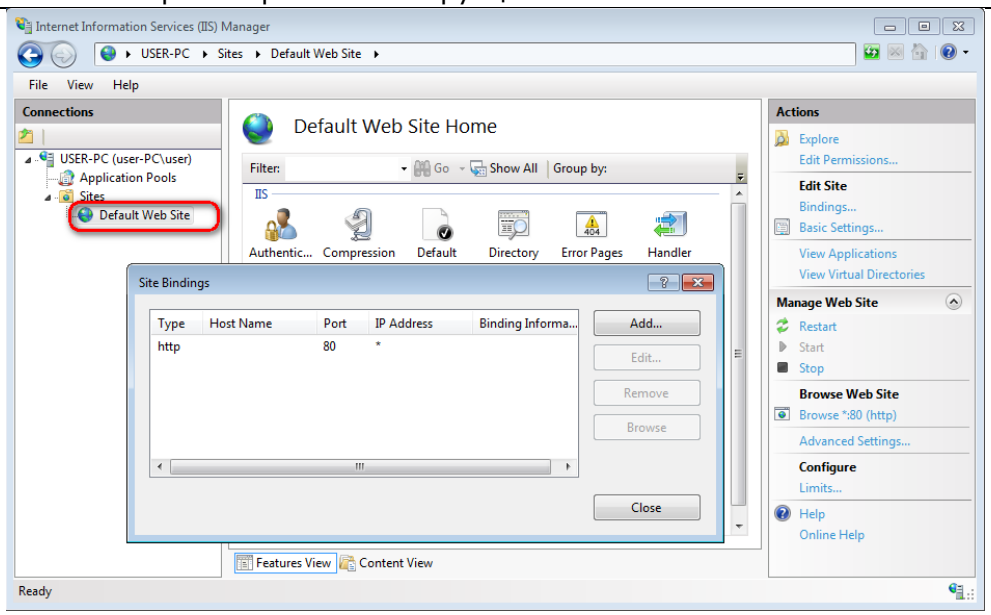


Рисунок 93. Диспетчер IIS

В списке привязок сайта нажмите кнопку Добавить… (Add…).

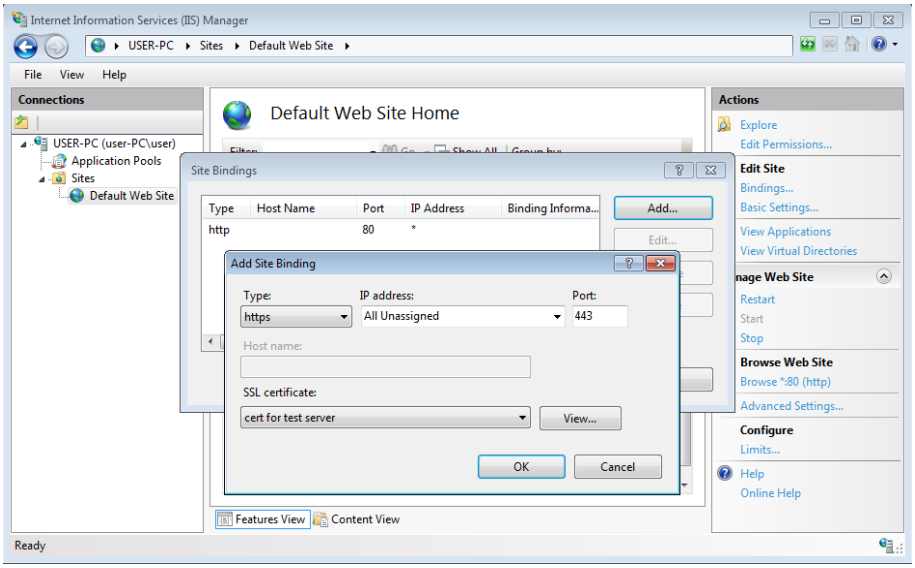


Рисунок 94. Добавление сертификата SSL

В открывшемся диалоге добавления привязки сайта укажите тип протокола подключения (Type) HTTPS, а в выпадающем списке Сертификаты SSL (SSL certificate) выберите сертификат, созданный для служб IIS. Нажмите OK для сохранения параметров, закройте Привязки сайта и перезапустите IIS, нажав Перезапустить (Restart) в окне диспетчера.

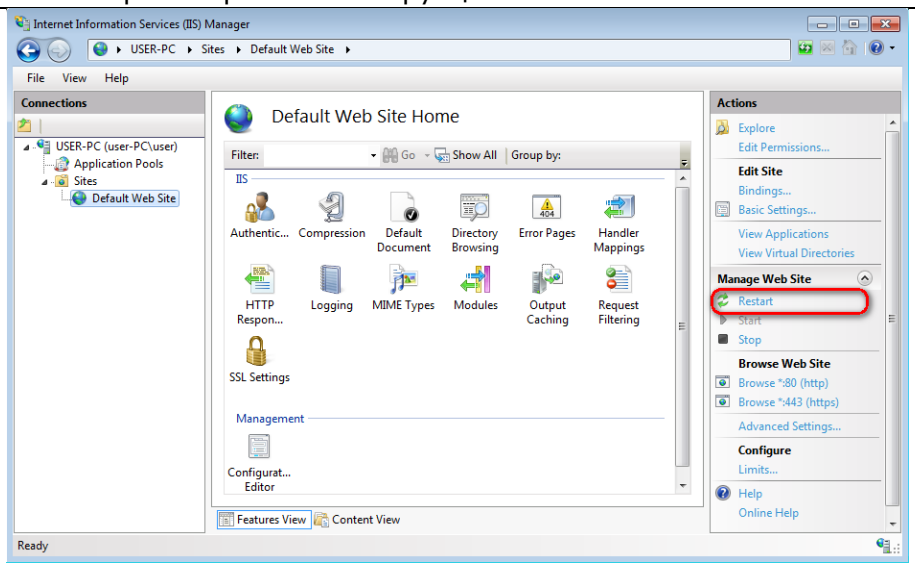


Рисунок 95. Перезапуск IIS

4.4.3. Проверка соединения по HTTPS

Для локальной проверки соединения используйте ссылку в левой части окна менеджера IIS, которая показана на следующем рисунке, или через браузер пройдите по ссылке https:/<domainname>// , где <domainname> – доменное имя настраиваемого сайта (где предварительно должен быть настроен DNS).

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).

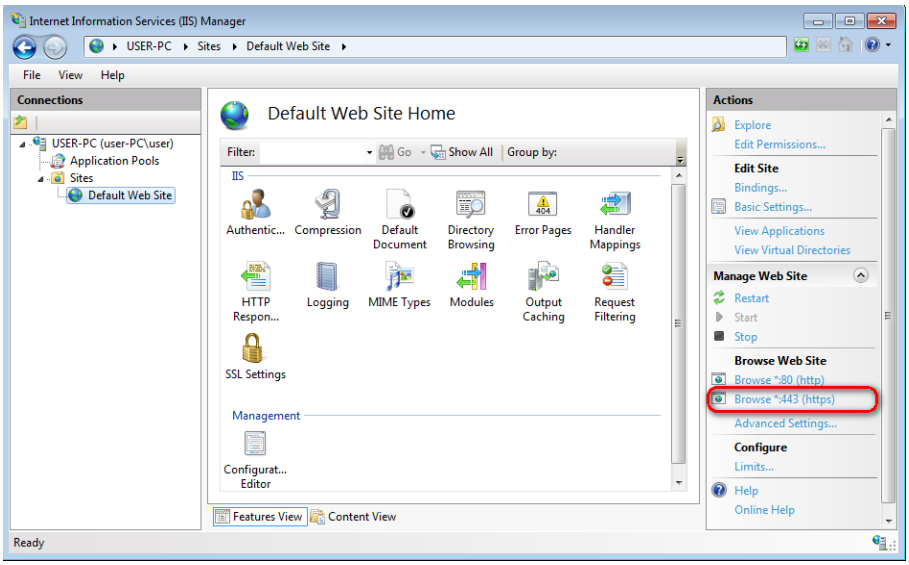


Рисунок 96. Проверка соединения с сервером по HTTPS

Если службы IIS настроены правильно, в браузере отобразится соответствующая страница:

Рисунок 97. 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).

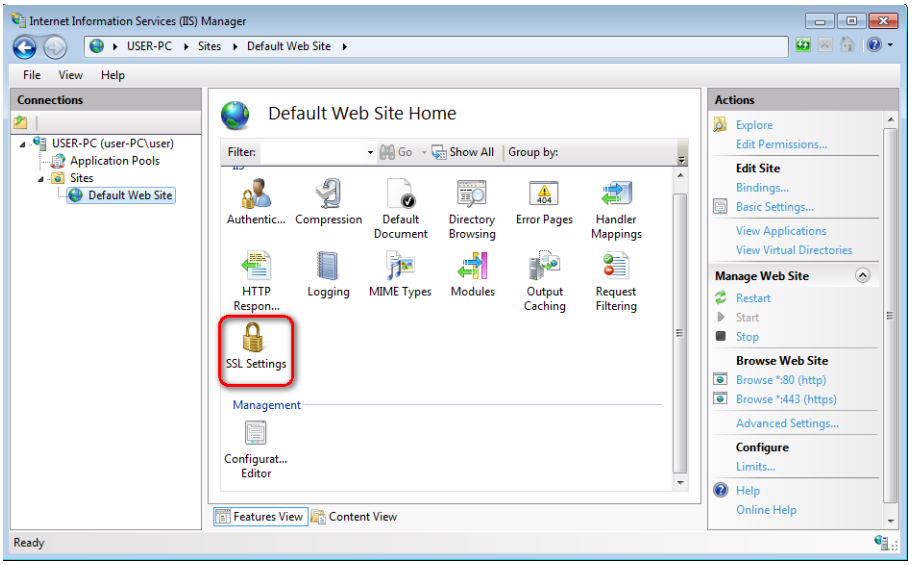


Рисунок 98. Настройка двусторонней аутентификации

В параметрах SSL проставьте флажок «Требовать SSL» (Require SSL) и укажите для сертификатов клиента «Требовать» (Require).

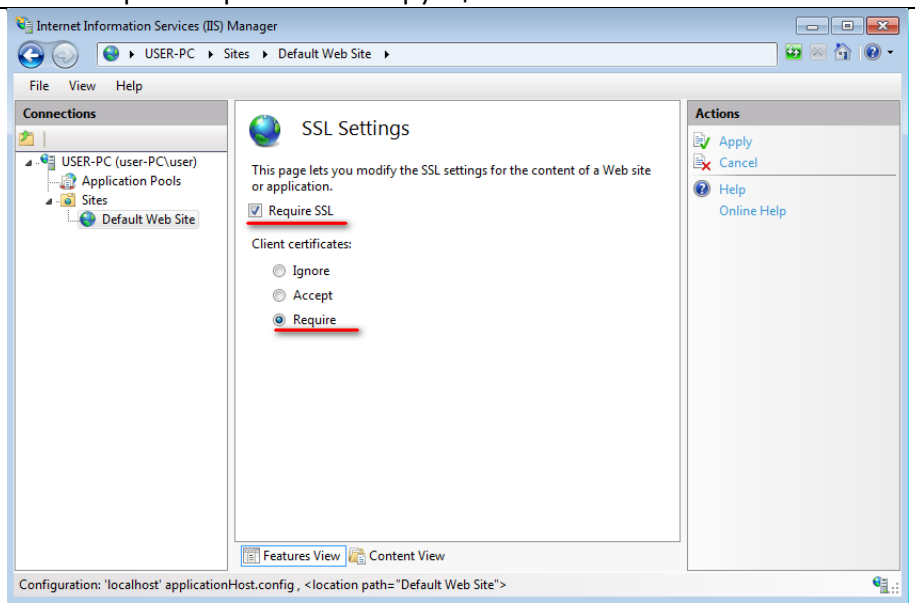


Рисунок 99. Параметры SSL для двусторонней аутентификации

После этого нажмите «Применить» (Apply) для сохранения изменений и перезапустите IIS описанным выше способом.

4.5. Установка личного сертификата пользователя

Для успешной работы пользователя с сервером по протоколу TLS, необходимо:

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. Для решения текущей задачи достаточно принять при установке параметры, рекомендуемые по умолчанию.

Сертификат пользователя можно получить через центр сертификации КриптоПро https://www.cryptopro.ru/certsrv/

На первой странице центра сертификации выберите «Сформировать ключи и отправить запрос на сертификат.

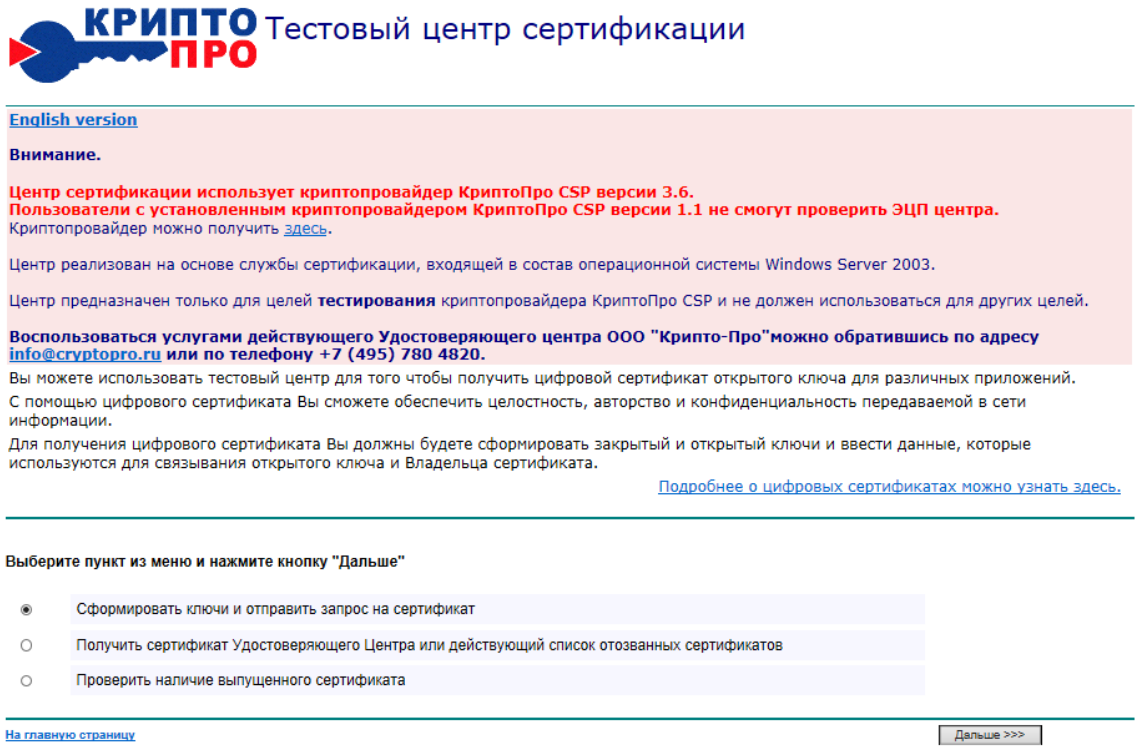


Рисунок 100. Запрос сертификата пользователя на тестовом ЦС

Далее следует выбрать ссылку «Создать и выдать запрос к этому ЦС»

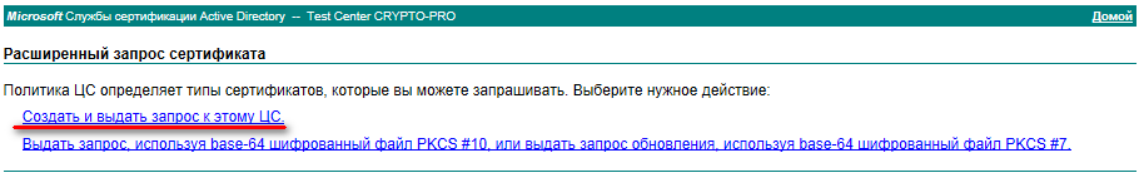


Рисунок 101. Расширенный запрос сертификата

В форме создания запроса обязательно заполните следующие параметры: имя пользователя, в качестве типа сертификата укажите сертификат проверки подлинности клиента, выберите CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider, при необходимости дальнейших манипуляций с ключом поставьте флажок «Пометить ключ как экспортируемый». Нажмите кнопку «Выдать».

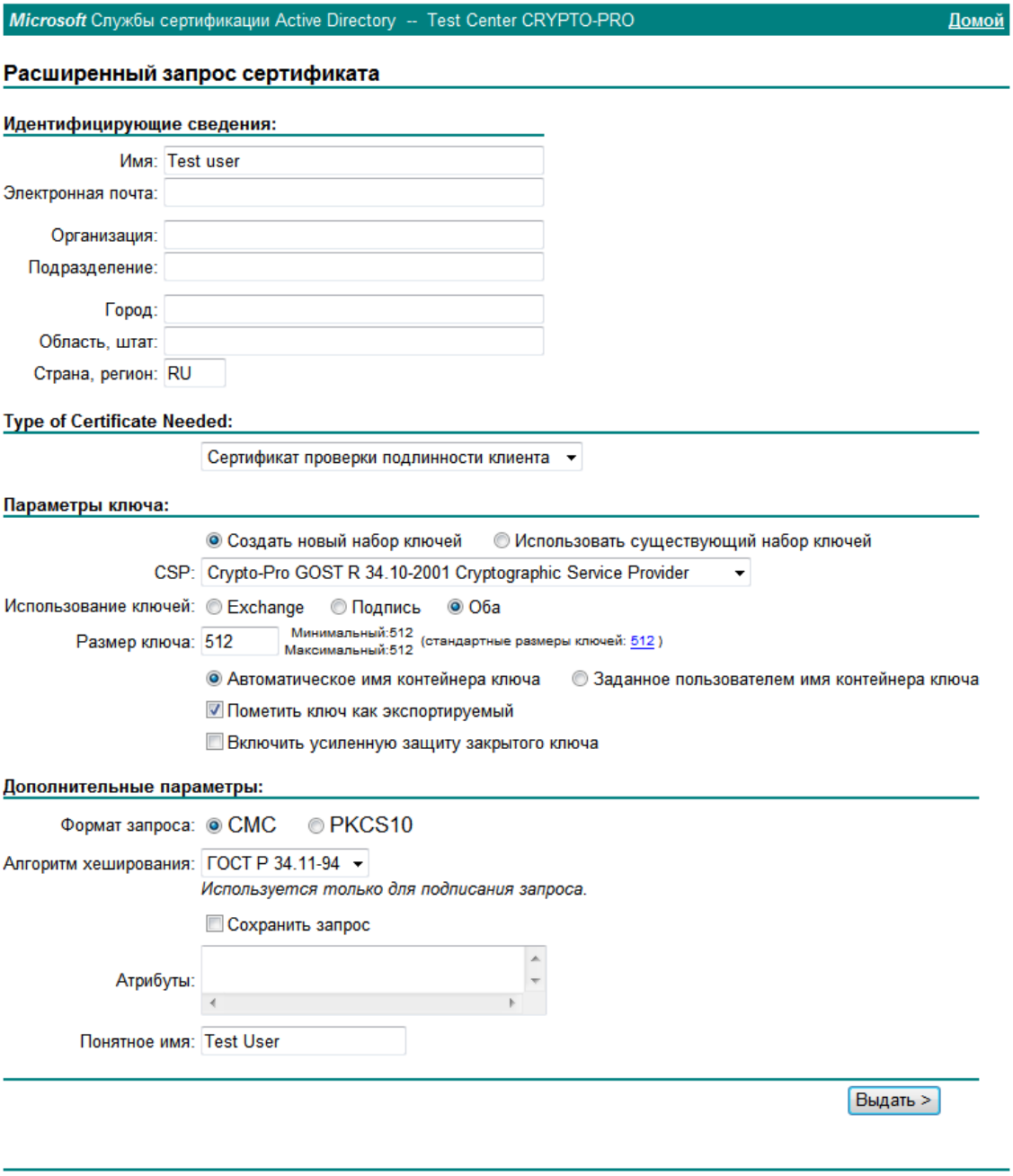


Рисунок 102. Параметры запроса сертификата пользователя

После срабатывания биологического датчика КриптоПро CSP предлагает задать пароль для создаваемого контейнера. Затем нужно установить выданный сертификат.

На открывшейся странице нажмите ссылку «Установить этот сертификат».

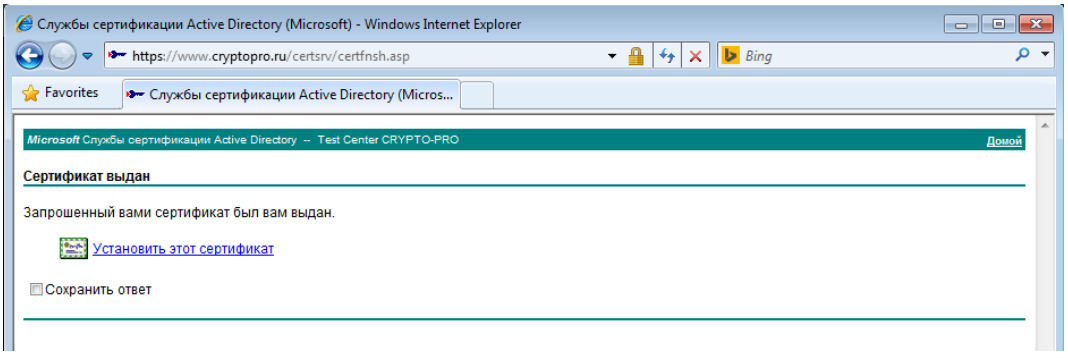


Рисунок 103. Установка сертификата в хранилище

При установке сертификата в хранилище текущего пользователя запрашивается пароль для контейнера. После ввода пароля сертификат установлен.

Проверить наличие сертификата в хранилище Личное текущего пользователя можно с помощью оснастки «Сертификаты».

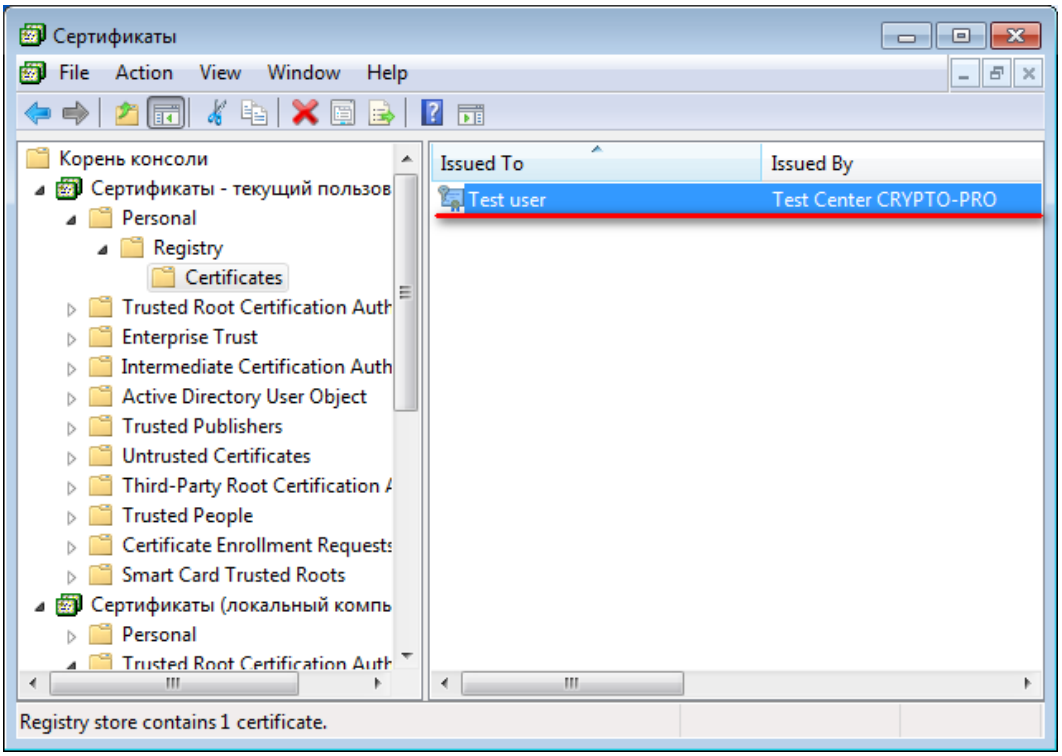


Рисунок 104. Проверка наличия сертификата пользователя в хранилище

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

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.

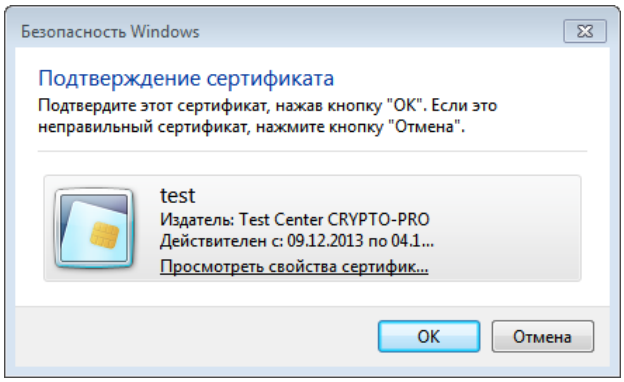


Рисунок 105. Выбор сертификата

После выбора сертификата будет запрошен пароль к контейнеру сертификата пользователя.

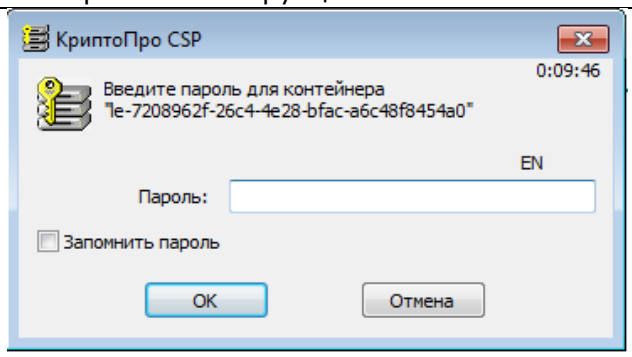


Рисунок 106. Ввод пароля контейнера закрытого ключа

При вводе правильного пароля пользователю открывается доступ к сайту.

Примечание. При получении сертификата пользователя необходимо убедиться в том, что поле «Улучшенный ключ» содержит значение «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)», а поле «Использование ключа» - 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.

5. Описание использования, настроек и управления ключами на сервере ISA/TMG

5.1. Размещение сертификата аутентификации сервера на сервере ISA/TMG

На компьютере с сервером ISA/TMG сертификат аутентификации сервера должен быть размещен в хранилище **Локальный компьютер\Личные** с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра сертификации, выдавшего этот сертификат - в хранилище **Локальный компьютер\Доверенные корневые Центры Сертификации** (если этот ЦС корневой) или **Локальный компьютер\Промежуточные Центры Сертификации** (если этот ЦС подчинённый. В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network Service** на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

Проверить наличие необходимых сертификатов можно с помощью оснастки "Сертификаты" – специально настроенной консоли MMC Windows. Для запуска консоли нужно выполнить **Пуск** ⇒ **Программы** ⇒ **КриптоПро** ⇒ **Сертификаты**

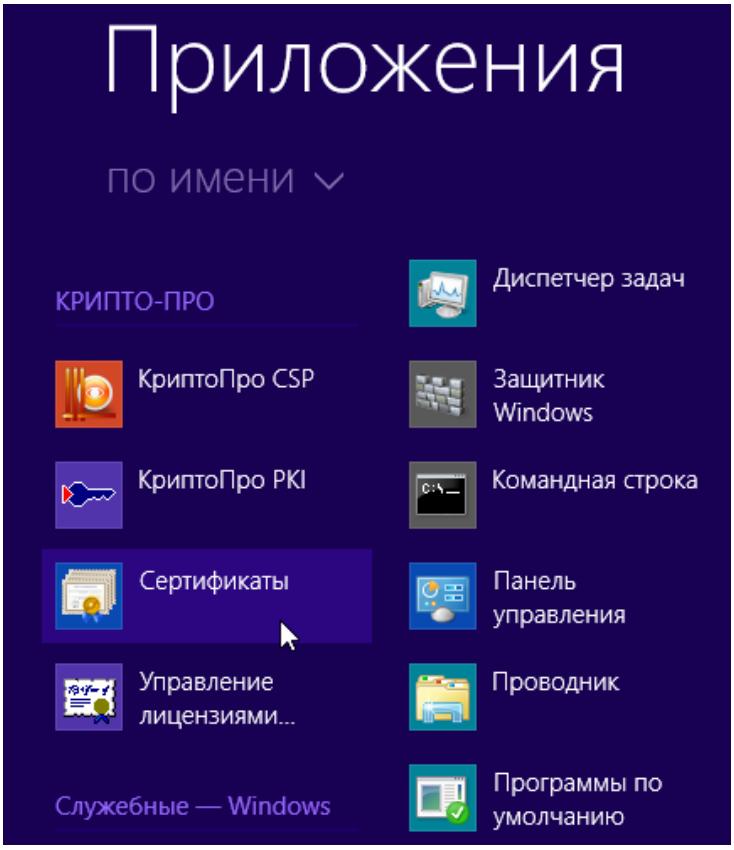


Рисунок 107. Запуск консоли Сертификаты

После запуска открывается консоль:

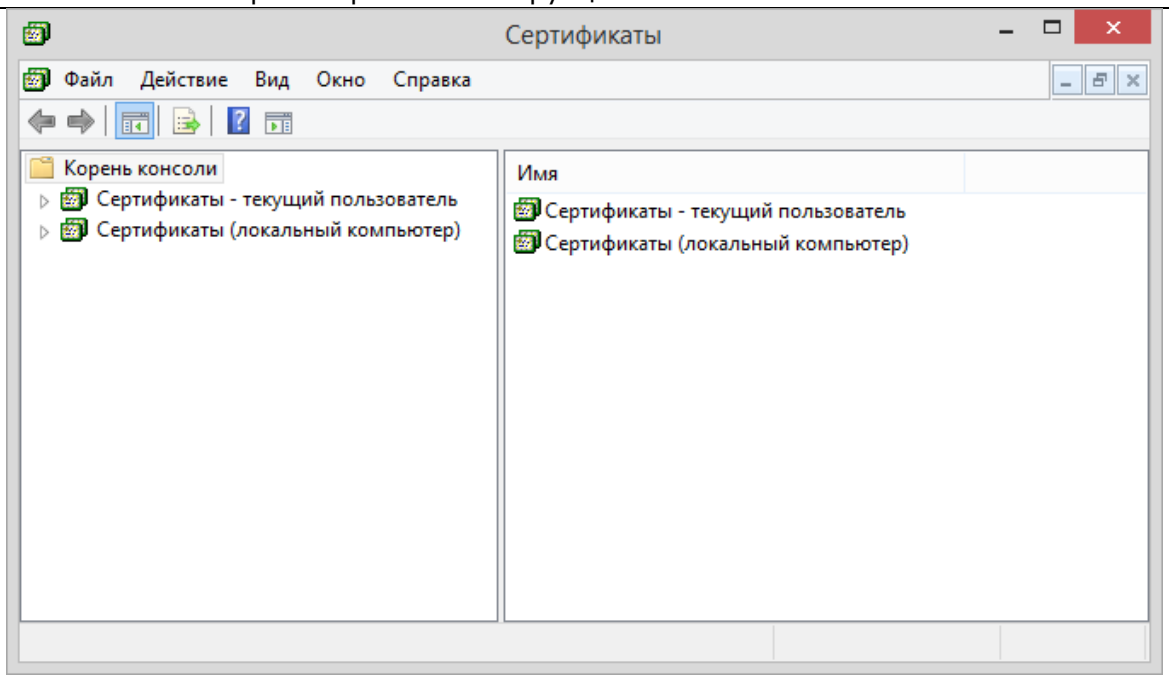


Рисунок 108. Корень консоли Сертификаты

Установите курсор на сертификат сервера ISA:

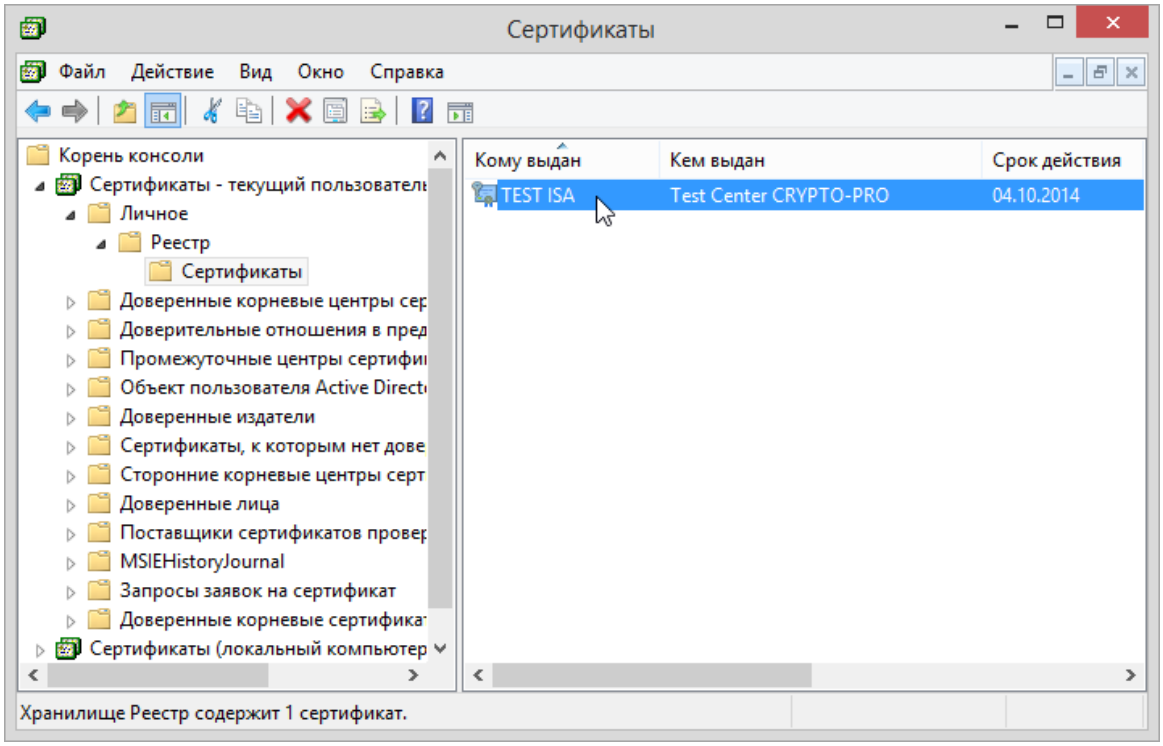


Рисунок 109. Хранилище Личное текущего пользователя

С использованием функции «Копировать», занесите сертификат в буфер обмена.

После этого установите курсор на разделе «Личные» сертификатов локального компьютера и выполните функцию «Вставить».

После установки сертификата серверной аутентификации ISA, таким же образом установите сертификат центра сертификации в хранилище «Доверенные корневые центры сертификации» хранилища локального компьютера.

5.2. Размещение сертификата клиентской аутентификации на сервере ISA/TMG

Если между сервером ISA/TMG и конечным веб-сервером требуется шифрование трафика по TLS с аутентификацией по сертификату клиента, то выпускается сертификат клиентской аутентификации. На компьютере с сервером ISA/TMG этот сертификат должен быть размещен в хранилище **Локальный компьютер\Личные** с привязкой к ключевому контейнеру локального компьютера. Сертификат Центра

сертификации, выдавшего этот сертификат - в хранилище **Локальный компьютер\Доверенные корневые Центры Сертификации** (если этот ЦС корневой) или **Локальный компьютер\Промежуточные Центры Сертификации** (если этот ЦС подчинённый. В этом случае все вышестоящие сертификаты промежуточных ЦС и корневой сертификат должны быть установлены в соответствующие хранилища локального компьютера).

Если ключевой контейнер, соответствующий этому сертификату, расположен в реестре компьютера, то необходимо добавить права на чтение-запись для служебной учётной записи **Network Service** на раздел реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys**

5.3. Настройка соединения с Web-клиентом

После установки сертификатов открытых ключей, необходимо установить и настроить Слушателя для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется на вкладке Incoming Web Requests окна свойств ISA сервера (Рисунок 110):

В окне ISA Management установить курсор на имя сервера и нажать правую кнопку мыши.

В появившемся меню выбрать пункт Properties.

В окне свойств сервера выбрать закладку Incoming Web Requests.

Выберите режим индивидуального Слушателя для каждого IP адреса в поле Identification.

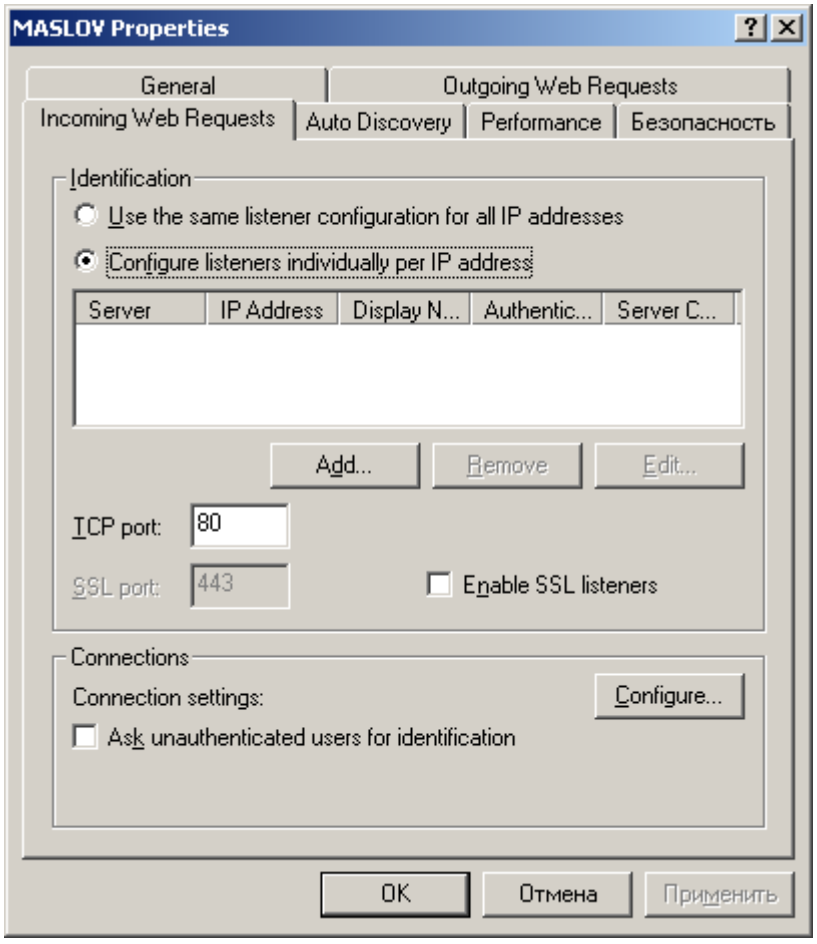


Рисунок 110. Установка и настройка Слушателей

Добавьте нового Слушателя в список слушателей ISA сервера.

Установите имя сервера.

Установите внешний IP-адрес, на который будет настроен Слушатель.

Введите имя, с которым будет отображаться данный Слушатель в дальнейшем (опционально).

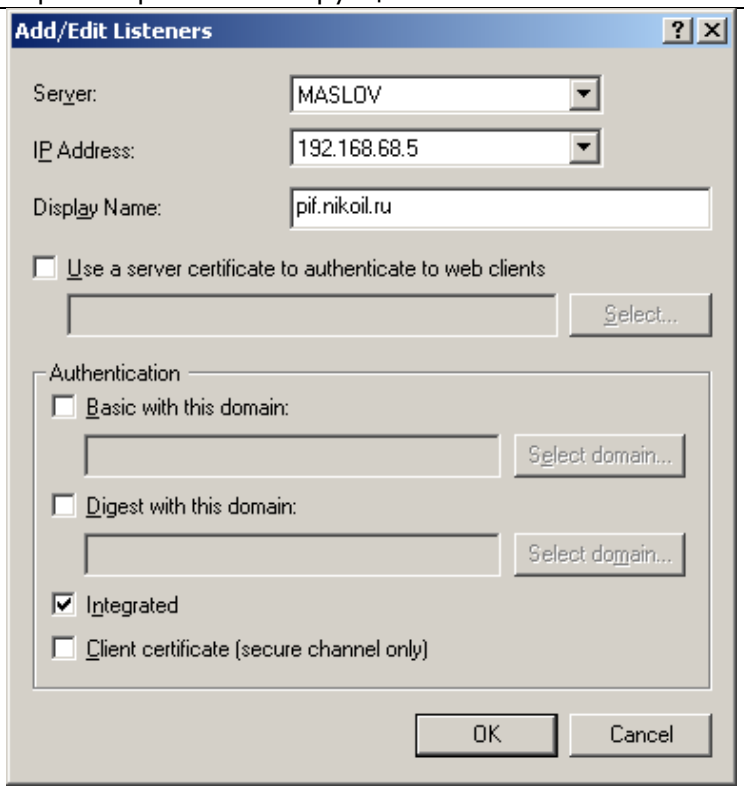


Рисунок 111. Добавление Слушателя/редактирование свойств Слушателя(1)

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификации сервера ISA необходимо:

В окне добавления Слушателя или в окне редактировании свойств Слушателя, указать на использование сертификата сервера при аутентификации с Web-клиентом.

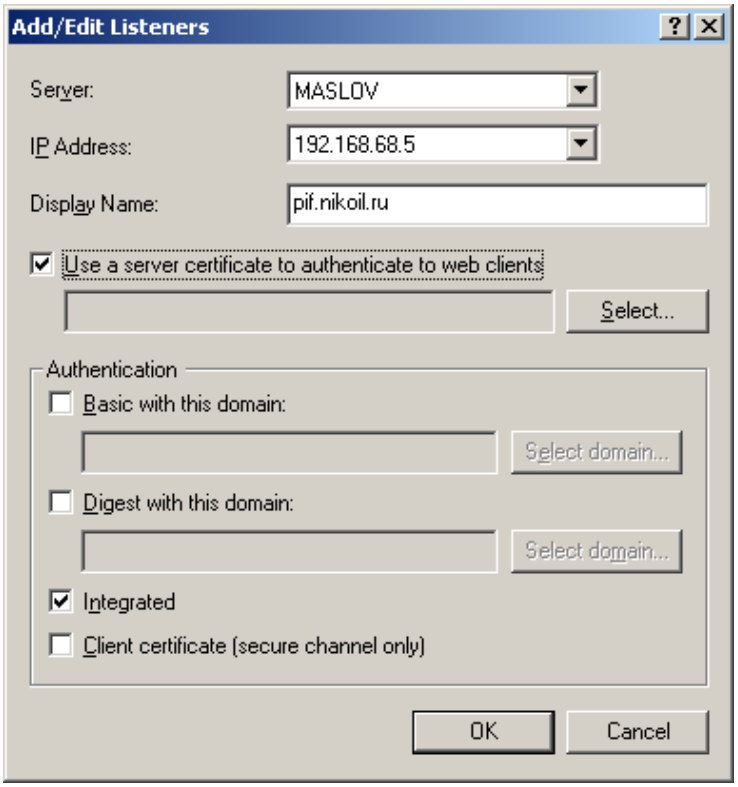


Рисунок 112. Добавление Слушателя/редактирование свойств Слушателя(2)

Выбрать сертификат сервера, который будет использоваться для аутентификации.

Нажать кнопку Select.

В появившемся окне выбрать из списка сертификат открытого ключа сервера:

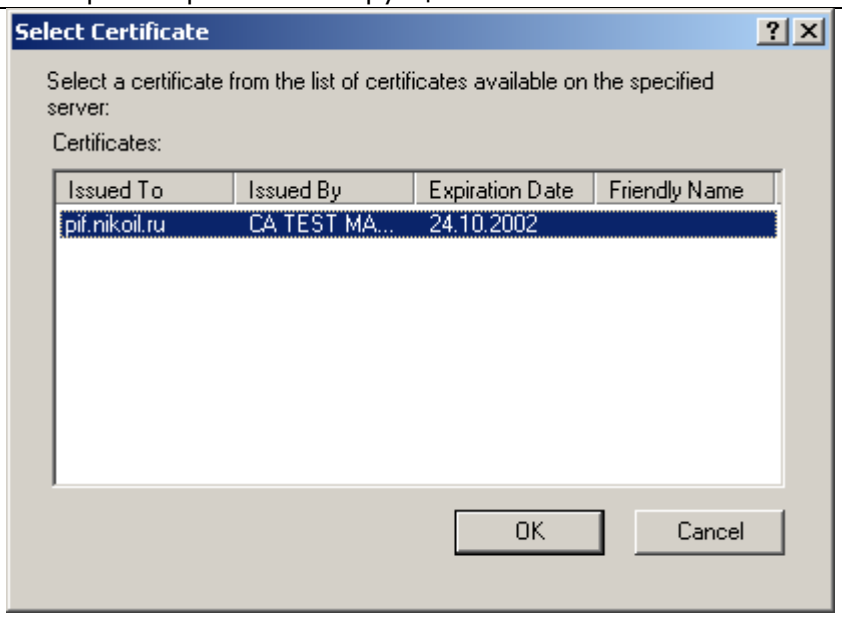


Рисунок 113. Выбор сертификата открытого ключа сервера

Указать на использование сертификата клиента (опция Client certificate (secure channel only)).

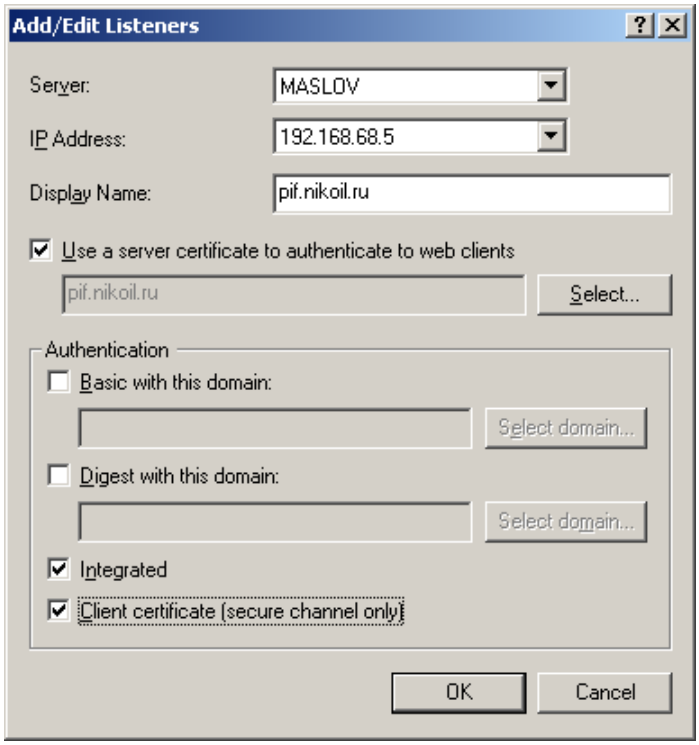


Рисунок 114. Добавление Слушателя/редактирование свойств Слушателя(3)

После установки сертификата (сертификатов) открытых ключей, необходимо установить и настроить Слушателя (Web listener) для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется по документации на ISA сервер.

В окне добавления Слушателя или в окне редактировании свойств Слушателя необходимо указать на использование сертификата сервера при аутентификации с Web-клиентом и выбрать настроенный в п. 3.5. сертификат сервера, который будет использоваться для аутентификации.

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификацией необходимо дополнительно указать на требование сертификата клиента.

5.4. Публикация Web-сервера в сети Интернет

В этом разделе рассматривается порядок действий при опубликовании Web-сервера, расположенного во внутренней сети. При этом соединение сервера ISA и Web-сервера будет установлено по протоколу SSL.

Для публикации Web-сервера во внешнюю сеть необходимо:

1. Получить и установить на публикуемый Web-сервер сертификат открытого ключа, который будет использоваться для серверной аутентификации.

Требования к сертификату:

- Имя сертификата (Common name) должно совпадать с доменным именем Web-сервера, указываемого для редиректа поступающих запросов (вкладка **Action** окна свойств правила Web публикации);
- Область использования ключа должна содержать «Аутентификация Сервера».

2. Установить сертификат корневого ЦС в цепочке сертификатов Web-сервера на сервере ISA, в хранилище **Локальный компьютер\Доверенные корневые Центры Сертификации.**
3. Настроить Web-сервер для поддержки SSL соединения.

Настройка Web-сервера производится в соответствии с документацией соответствующего Web-сервера.

4. Создать и настроить правила публикации на сервере ISA.

В окне **ISA Management** установить курсор на **Web Publishing Rules,** находящийся в группе **Publishing**

Нажать правую кнопку мыши и в появившемся меню выбрать последовательно **New** и **Rule**

В открывшемся окне, с помощью Мастера создания Правила Web публикации, создать правило.

Ввести имя публикации (произвольное имя) и нажать «Далее»

Рисунок 115. Окно Мастера создания Правила Web

В окне **Destination Sets** оставить значение, предлагаемое по умолчанию (любые назначения) и нажать «Далее».

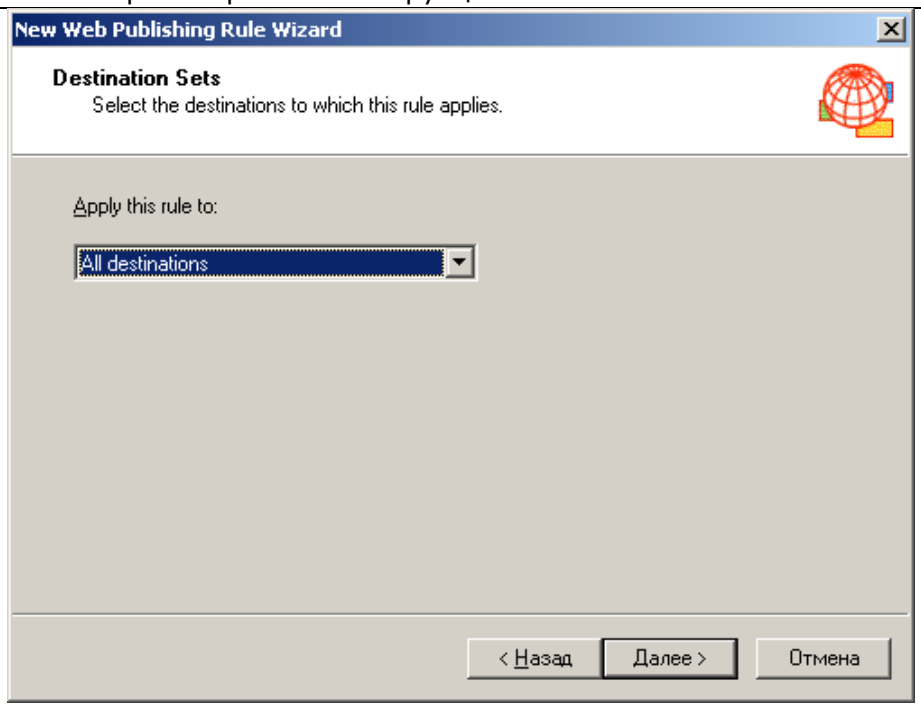


Рисунок 116. Окно установки назначения

Этой установкой определяется, что данное правило публикации (фактически редирект) будет применяться ко всем Web-запросам, прошедшим через Слушателей, вне зависимости от того, какой ресурс из внутренней сети они запросили. В случае публикации нескольких Web-серверов, необходимо создать и применять в правилах публикации назначения.

В окне Client Type оставить значение, предлагаемое по умолчанию (любые запросы) и нажать «Далее»

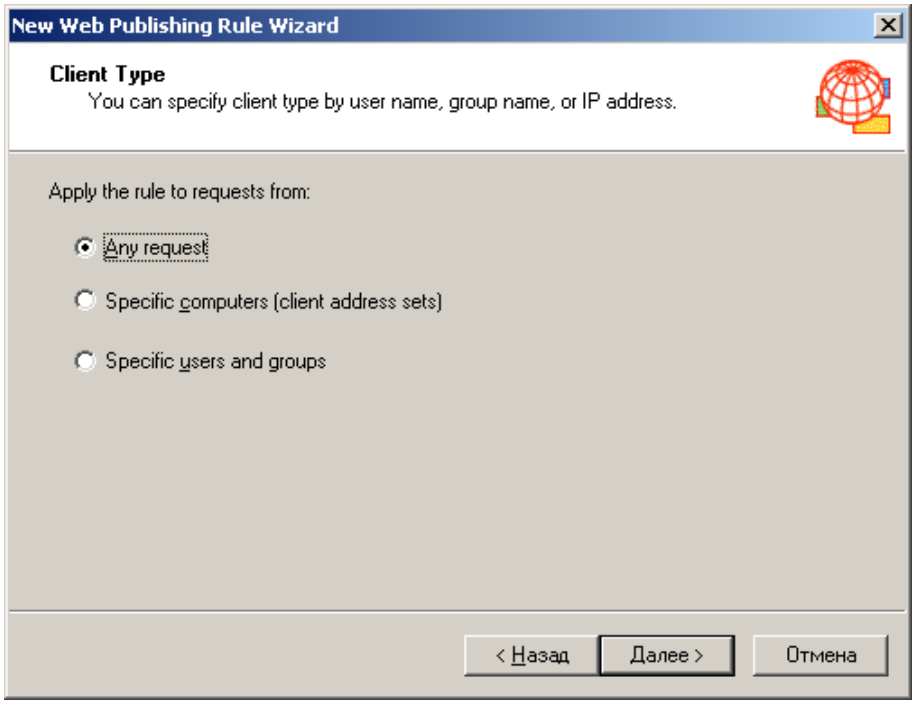


Рисунок 117. Окно типа клиента

В этом окне мы указываем, что правило применяется ко всем Web-запросам, вне зависимости от того клиента, кто сформировал запрос.

В окне **Rule Action** выбрать редирект запросов во внутренний Web-сервер (**Redirect the request to this ...**)

Ввести доменное имя публикуемого Web-сервера и нажать «Далее».

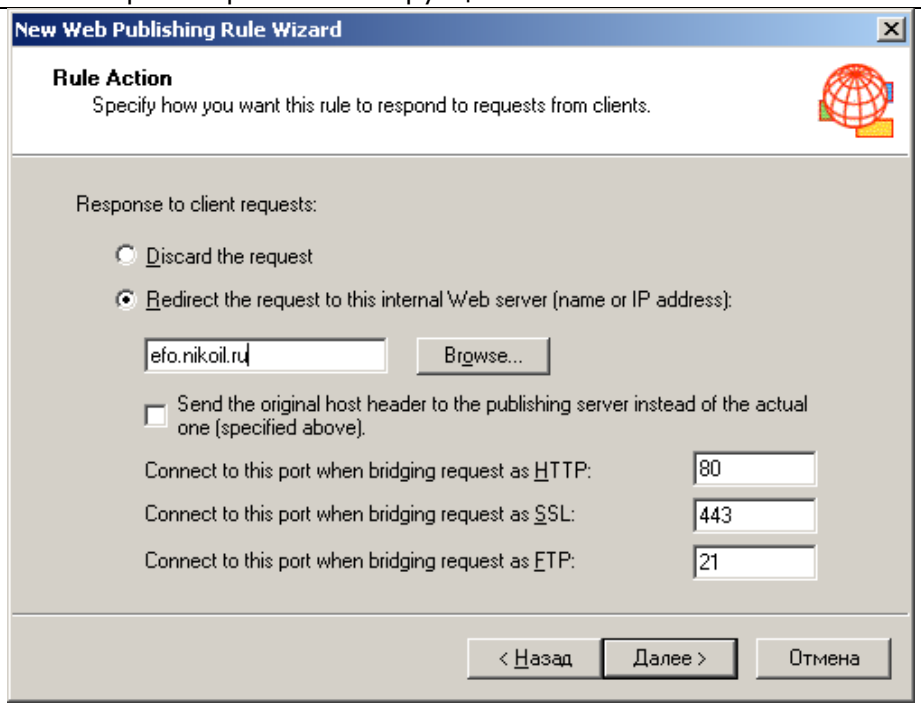


Рисунок 118. Окно ввода доменного имени

Установив правило редиректа таким образом, все запросы, пришедшие к Слушателю на 80 порт, будут редиректироваться на 80 порт Web-сервера. Тоже самое будет происходить с запросами, поступившими на 443 порт (по протоколу TLS).

Завершить работу Мастера, нажав «Готово».

В списке правил Web-публикации появится новая строка, соответствующая созданному нами правилу.

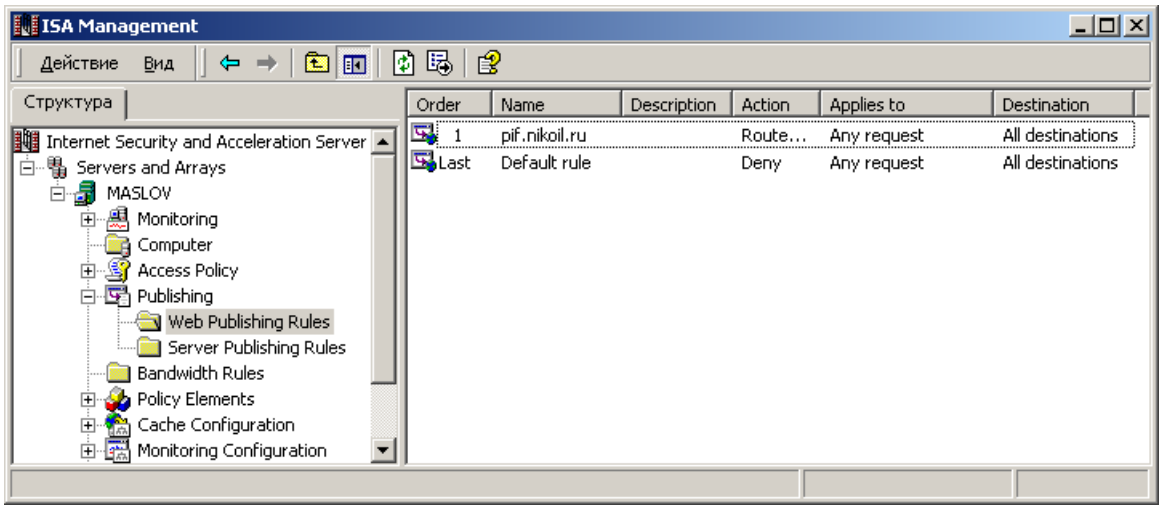


Рисунок 119. Список правил Web-публикации

6. 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. ссылку на раздел в инструкции).

6.1. Установка и настройка службы сертификации Active Directory (ЦС)

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**.

На шаге выбора роли сервера необходимо отметить **Службы сертификатов Active Directory**.

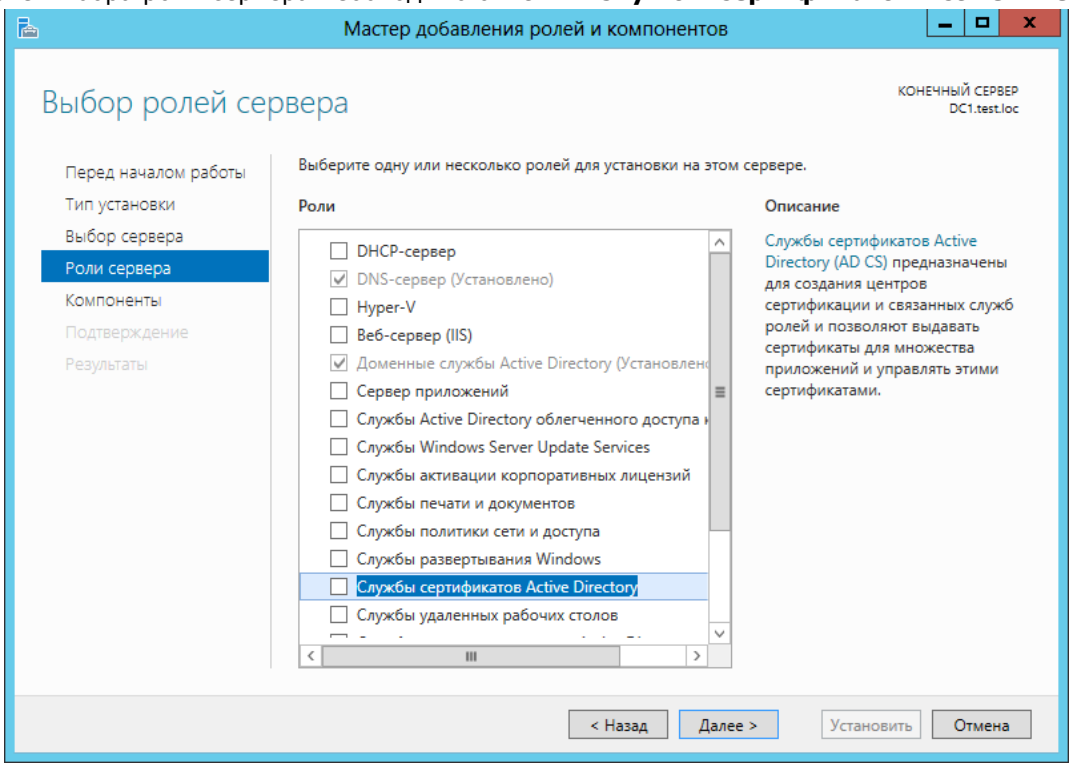


Рисунок 120. Добавление роли ЦС

При этом добавляются необходимые компоненты:

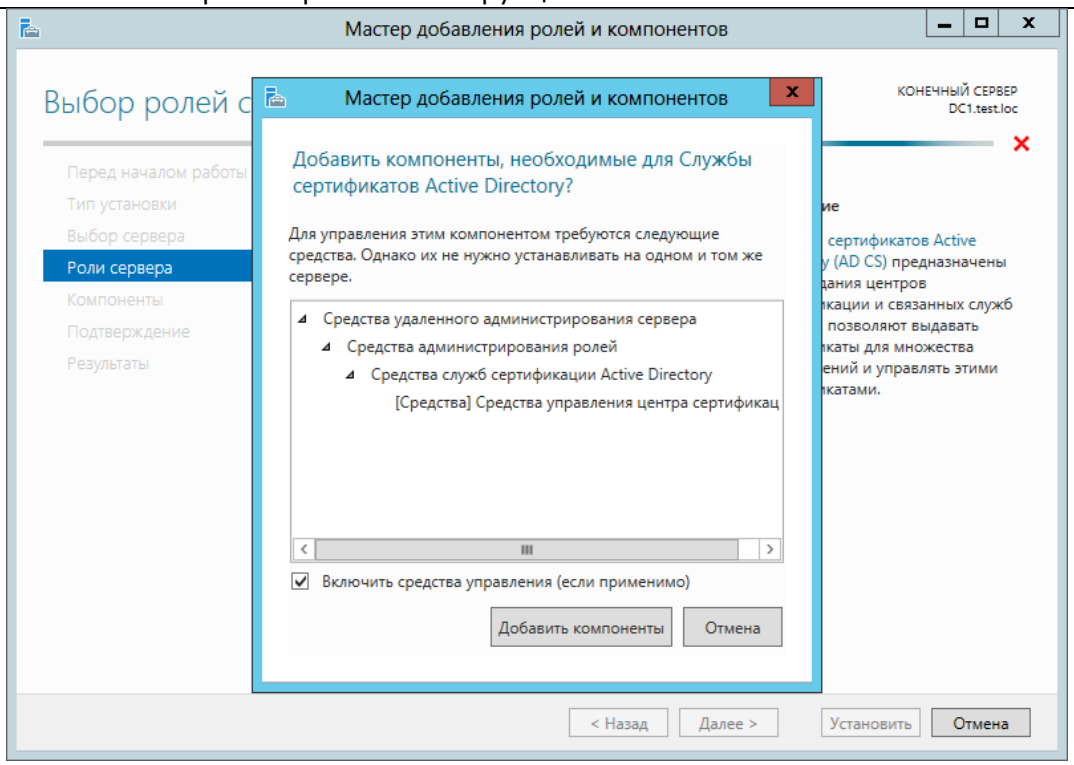


Рисунок 121. Добавление компонентов для роли ЦС

Далее принимаются по умолчанию компоненты и на следующем шаге выбирается служба ролей **Центр сертификации**.

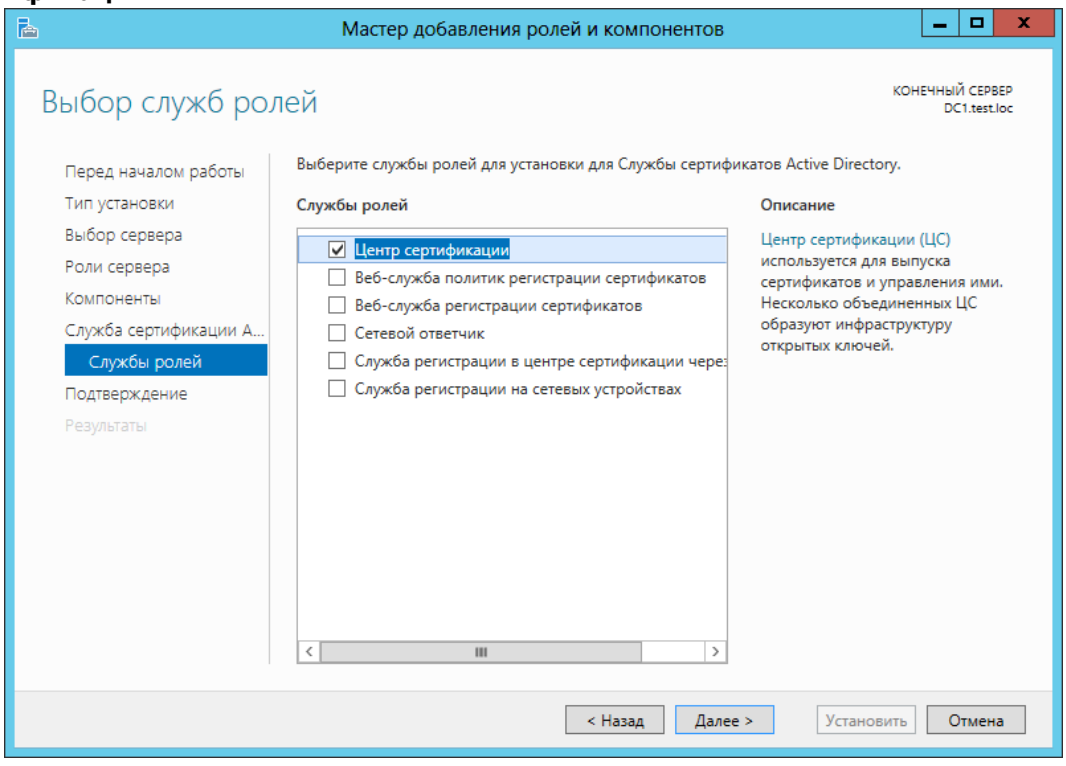


Рисунок 122. Выбор службы роли ЦС

На шаге **Подтверждение** после просмотра выбранных для установки компонентов нажмите кнопку **Установить**.

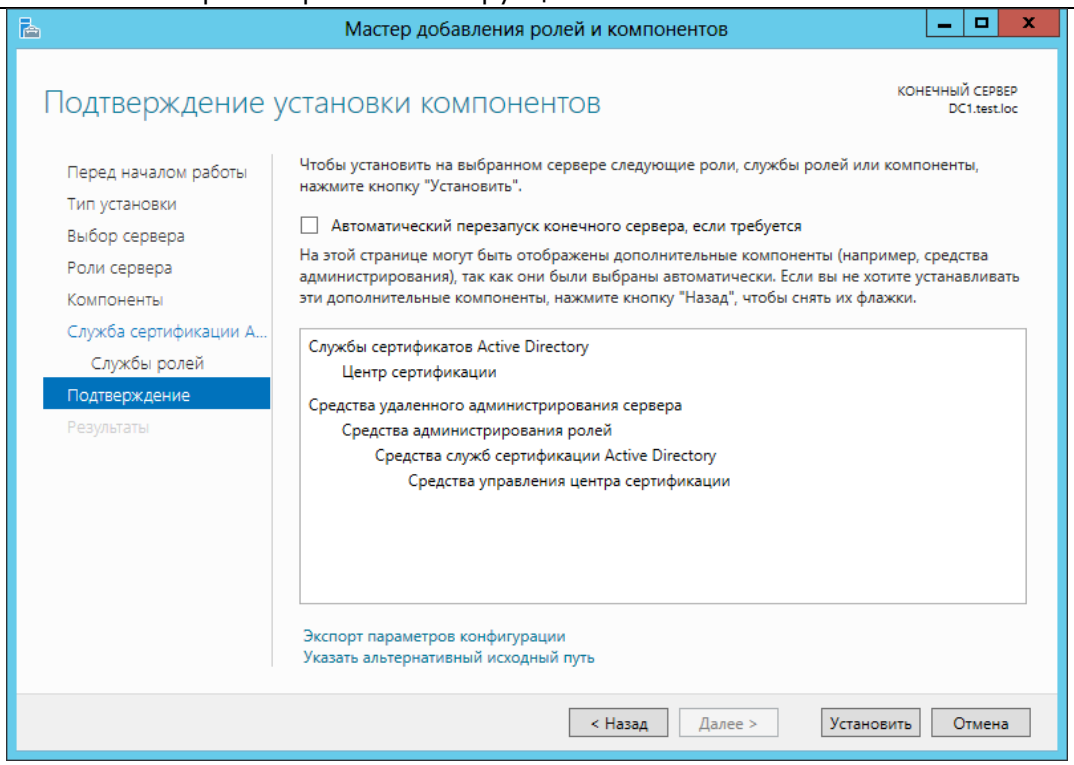


Рисунок 123. Подтверждение установки компонентов роли ЦС

По окончании установки компонентов, требующихся для роли Центра сертификации нужно настроить службы сертификатов. Для этого нажмите «Настроить службы сертификатов Active Directory на конечном сервере».

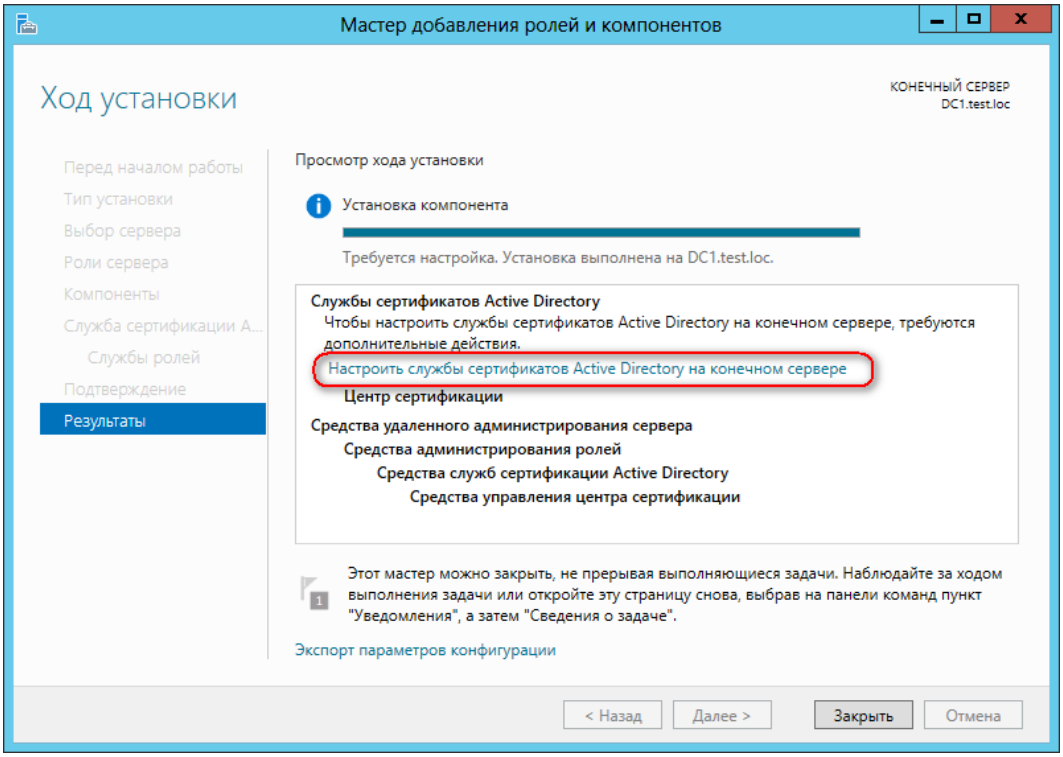


Рисунок 124. Настройка службы сертификатов AD на конечном сервере

Откроется мастер настройки конфигурации службы сертификатов.

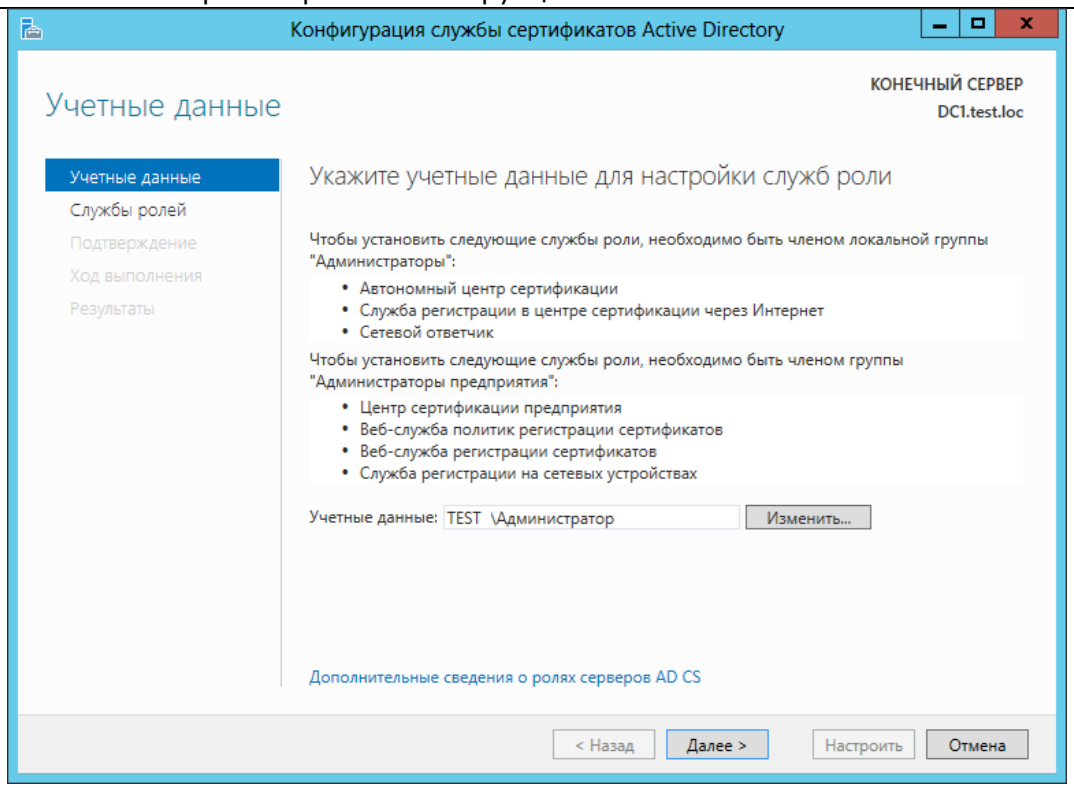


Рисунок 125. Учетные данные службы сертификатов AD

Укажите учетные данные для настройки и на следующем шаге выберите роль «Центр сертификации».

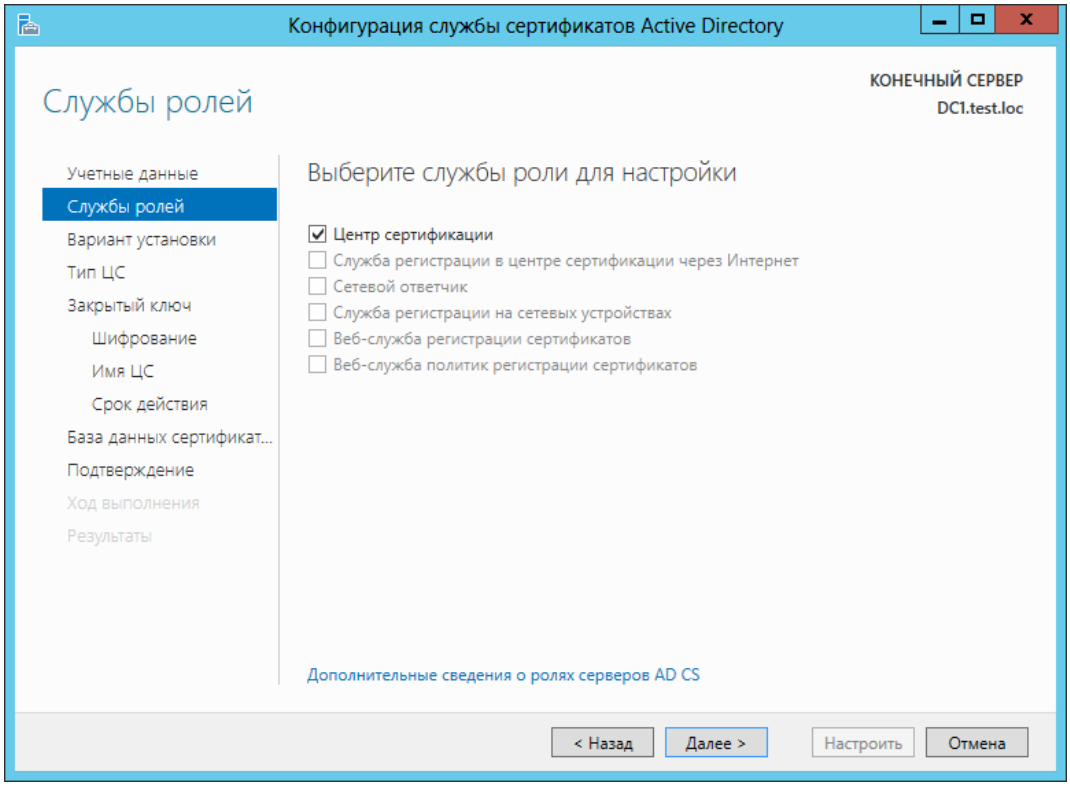


Рисунок 126. Выбор службы роли для настройки ЦС

Нажмите Далее и выберите вариант установки.

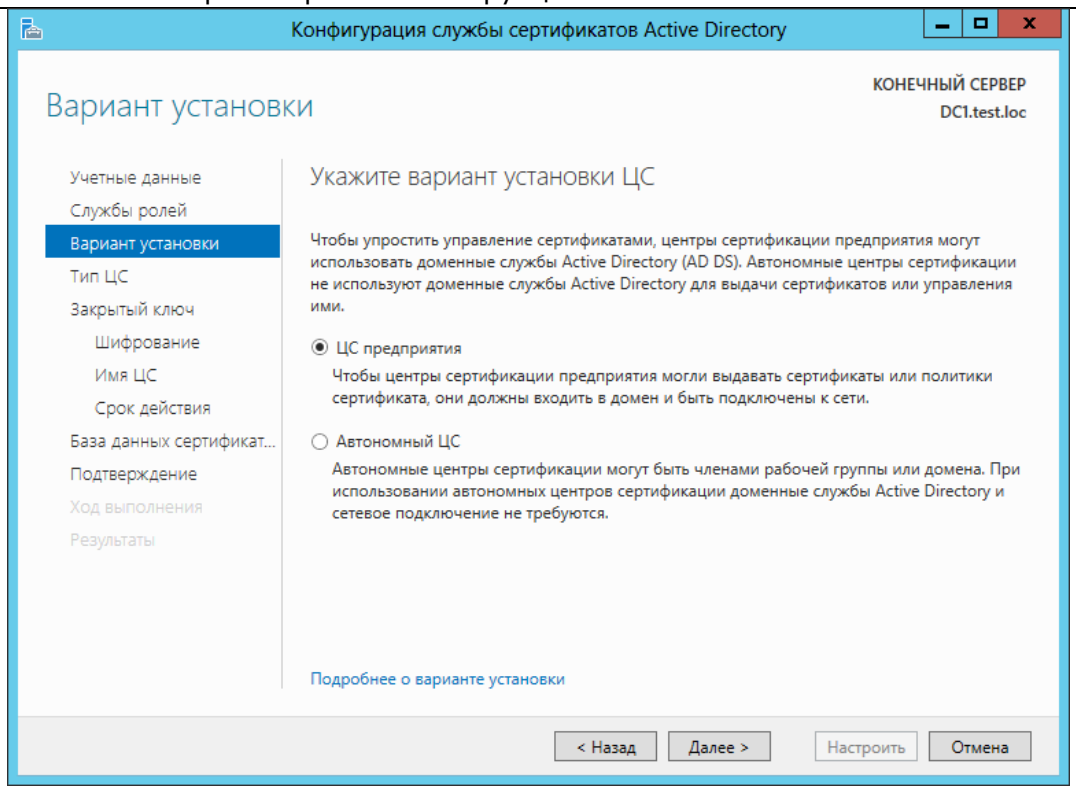


Рисунок 127. Выбор варианта установки ЦС

На следующем шаге укажите тип ЦС (корневой/подчиненный).

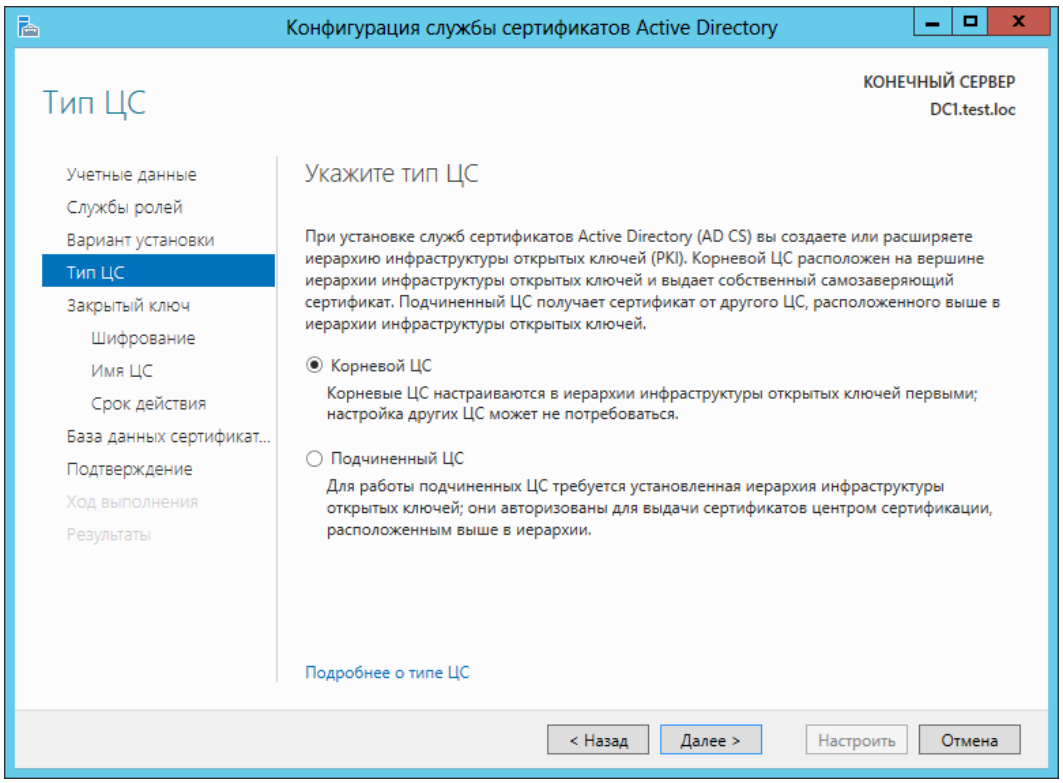


Рисунок 128. Выбор типа ЦС

После этого нужно создать закрытый ключ ЦС.

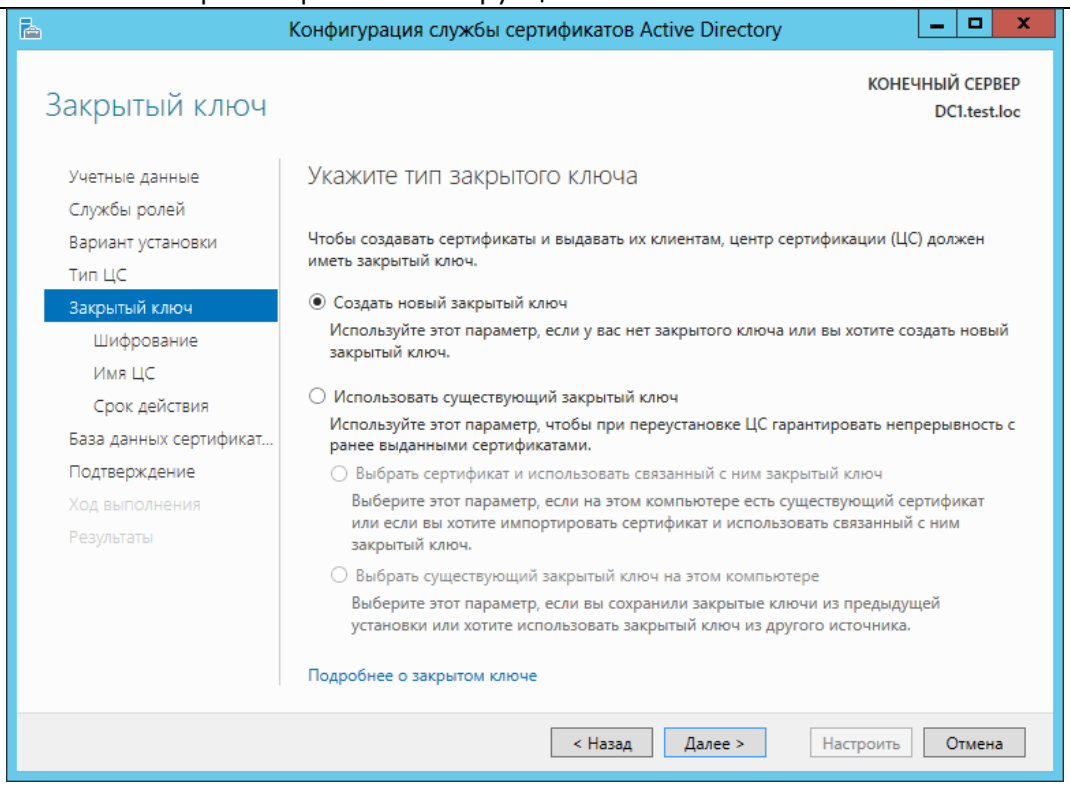


Рисунок 129. Выбор типа закрытого ключа для ЦС

Далее выберите из доступного списка поставщика служб шифрования и проставьте флажок «Разрешить взаимодействие с администратором, если ЦС обращается к закрытому ключу».

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

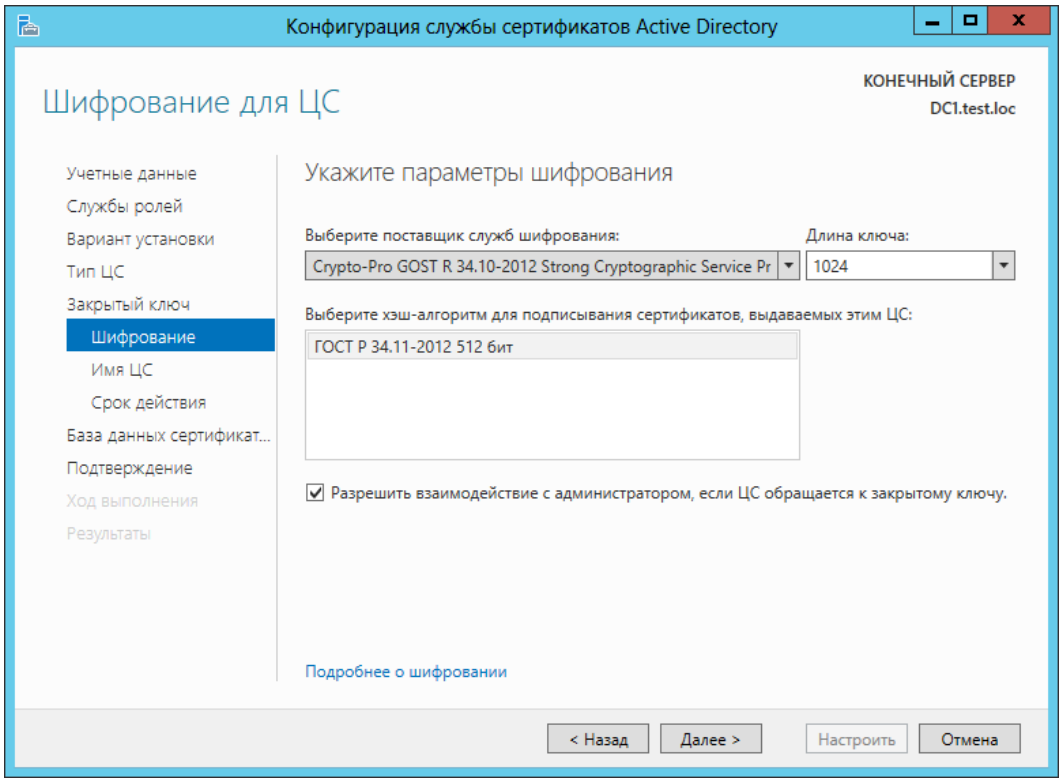


Рисунок 130. Выбор параметров шифрования для ЦС

На следующем шаге задается имя ЦС.

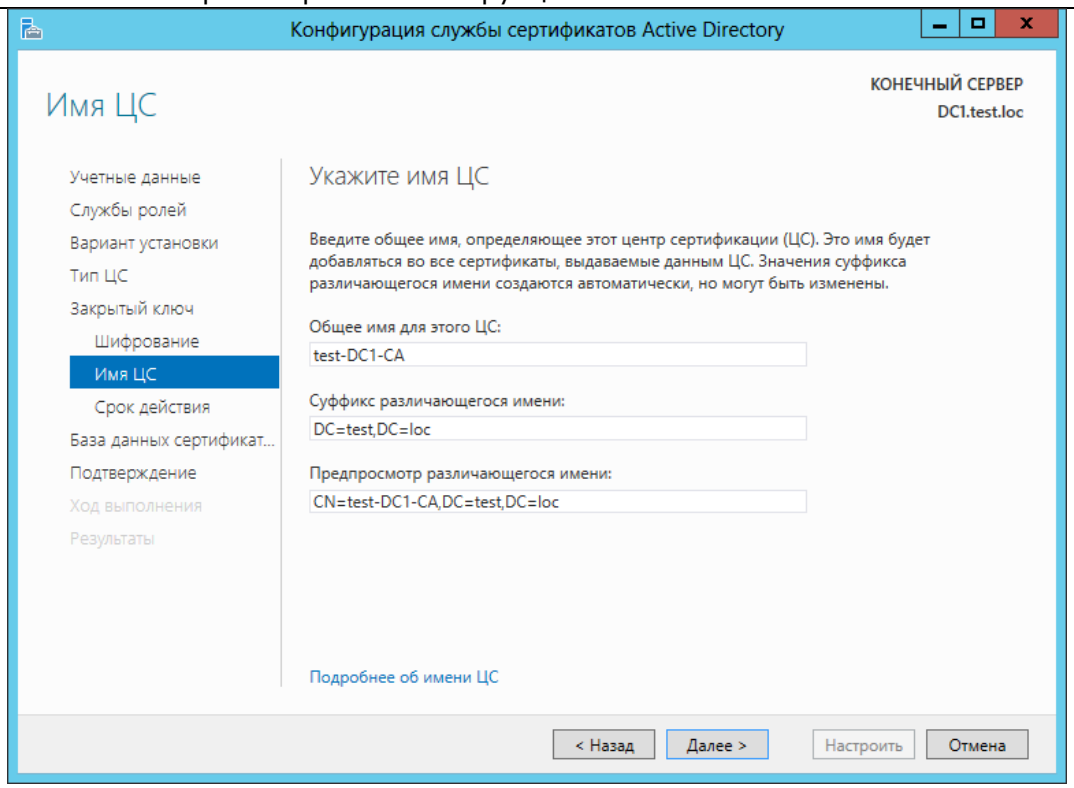


Рисунок 131. Ввод общего имени ЦС

После этого указывается срок действия ключа и расположение базы данных сертификатов.

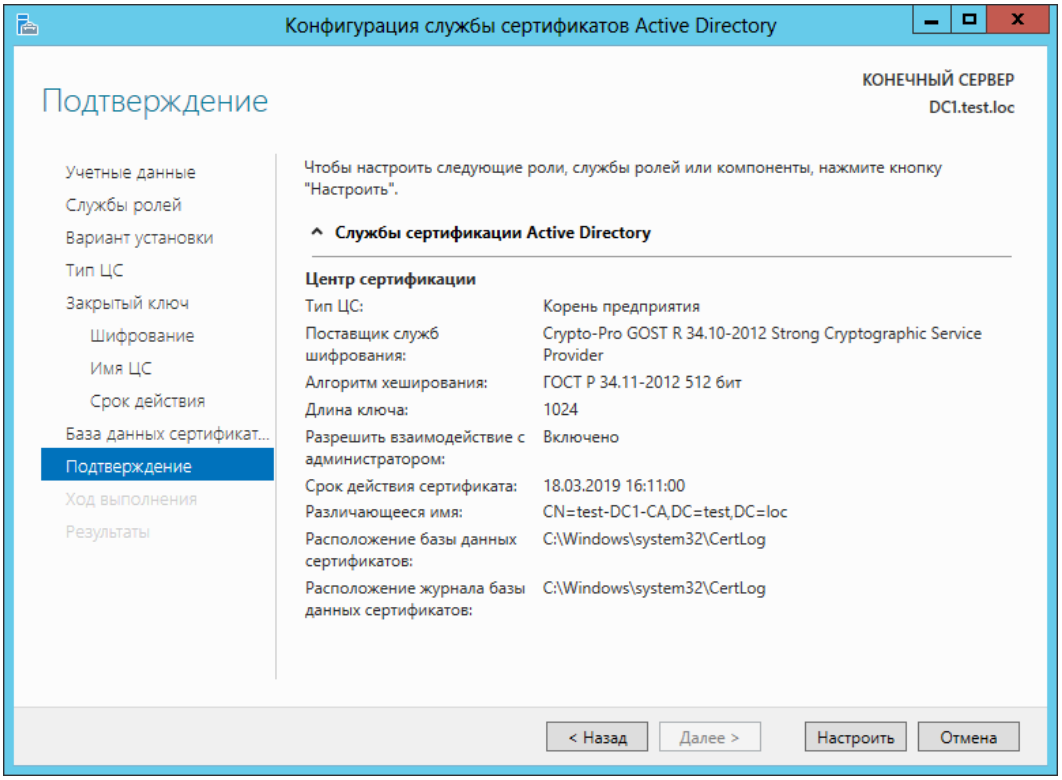


Рисунок 132. Подтверждение параметров ЦС

Все указанные параметры ещё раз выводятся на шаге **Подтверждение**. Нажмите **Настроить** для того, чтобы сконфигурировать службы в соответствии с этими параметрами.

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

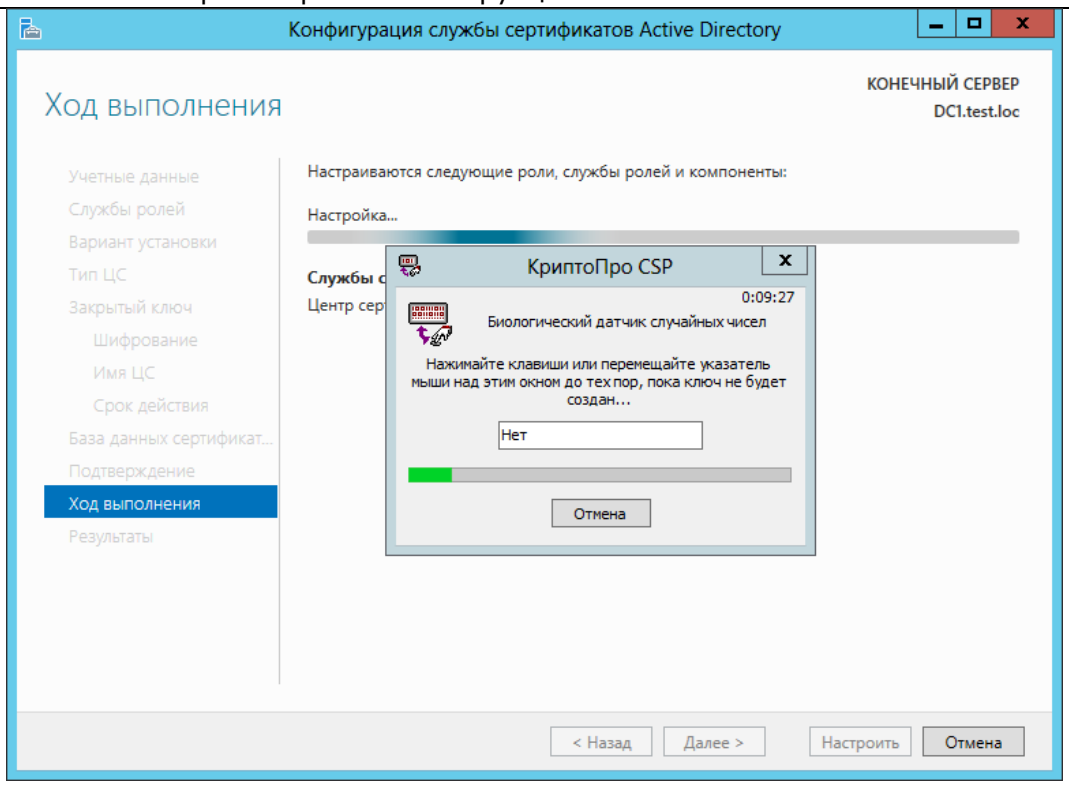


Рисунок 133. Выполнение конфигурирования ЦС

По окончании выполнения конфигурирования выводится информация об успешной настройке службы ЦС.

После выполнения данной задачи корневой сертификат ЦС можно увидеть в хранилище **Доверенные корневые центры Локального компьютера** через оснастку **Сертификаты**.

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

6.2. 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, нужно 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: **Панель управления – Администрирование – Центр Сертификации**. В список шаблонов сертификатов необходимо включить шаблоны:

Контроллер домена,

Агент регистратор,

Вход со смарт-картой.

Для этого выберите **Шаблоны сертификатов**, затем из контекстного меню **Создать – Выдаваемый шаблон сертификата**.

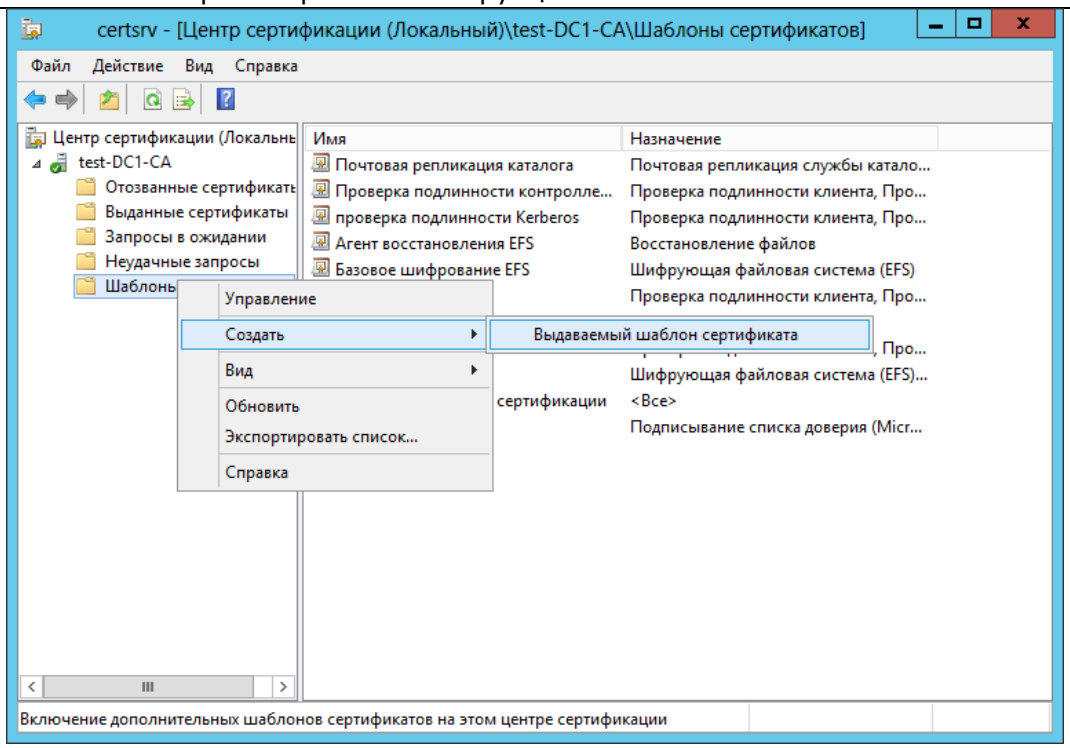


Рисунок 134. Добавление шаблонов сертификатов

Откроется окно включения шаблонов сертификатов, в котором нужно выделить шаблоны и нажать **ОК**.

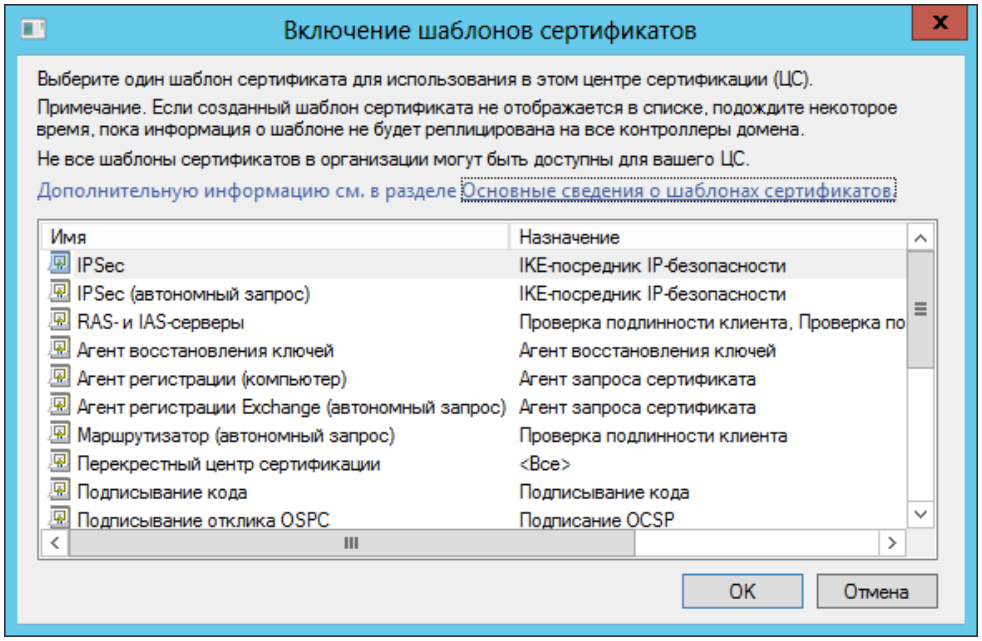
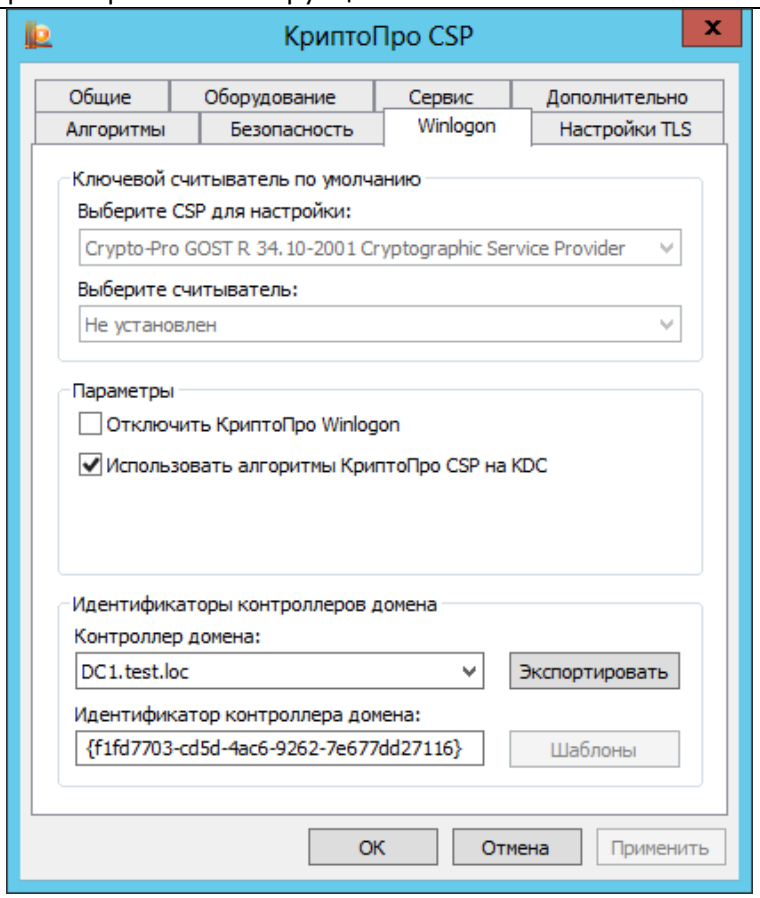


Рисунок 135. Включение шаблонов сертификатов

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



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.

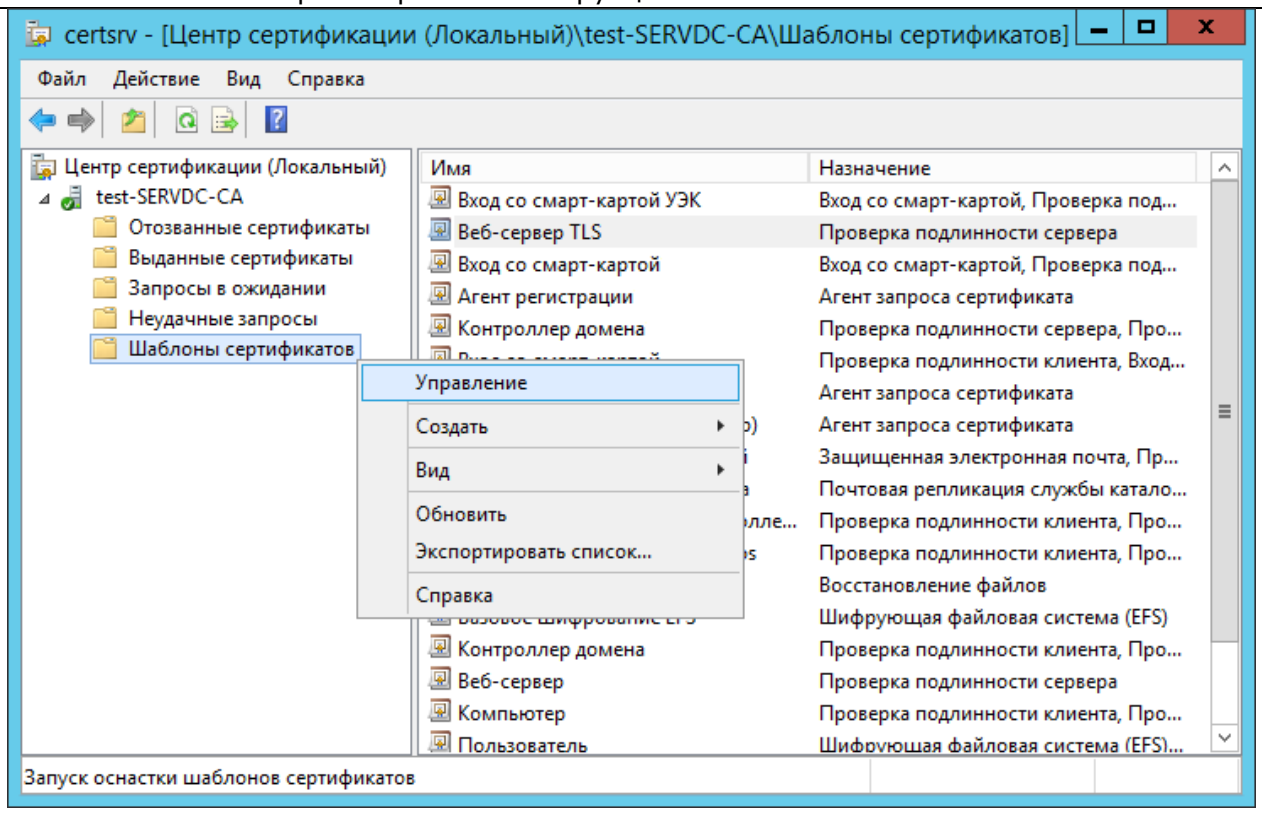
6.2.1. Настройка шаблонов сертификатов

Для того, чтобы сертификаты можно было использовать в Winlogon, нужно, чтобы они удовлетворяли определённым требованиям к сертификатам Контроллера домена, Агента регистратора, Входа по смарт-карте. Подробнее данные требования описаны в документации Microsoft http://support.microsoft.com/kb/281245/en-us

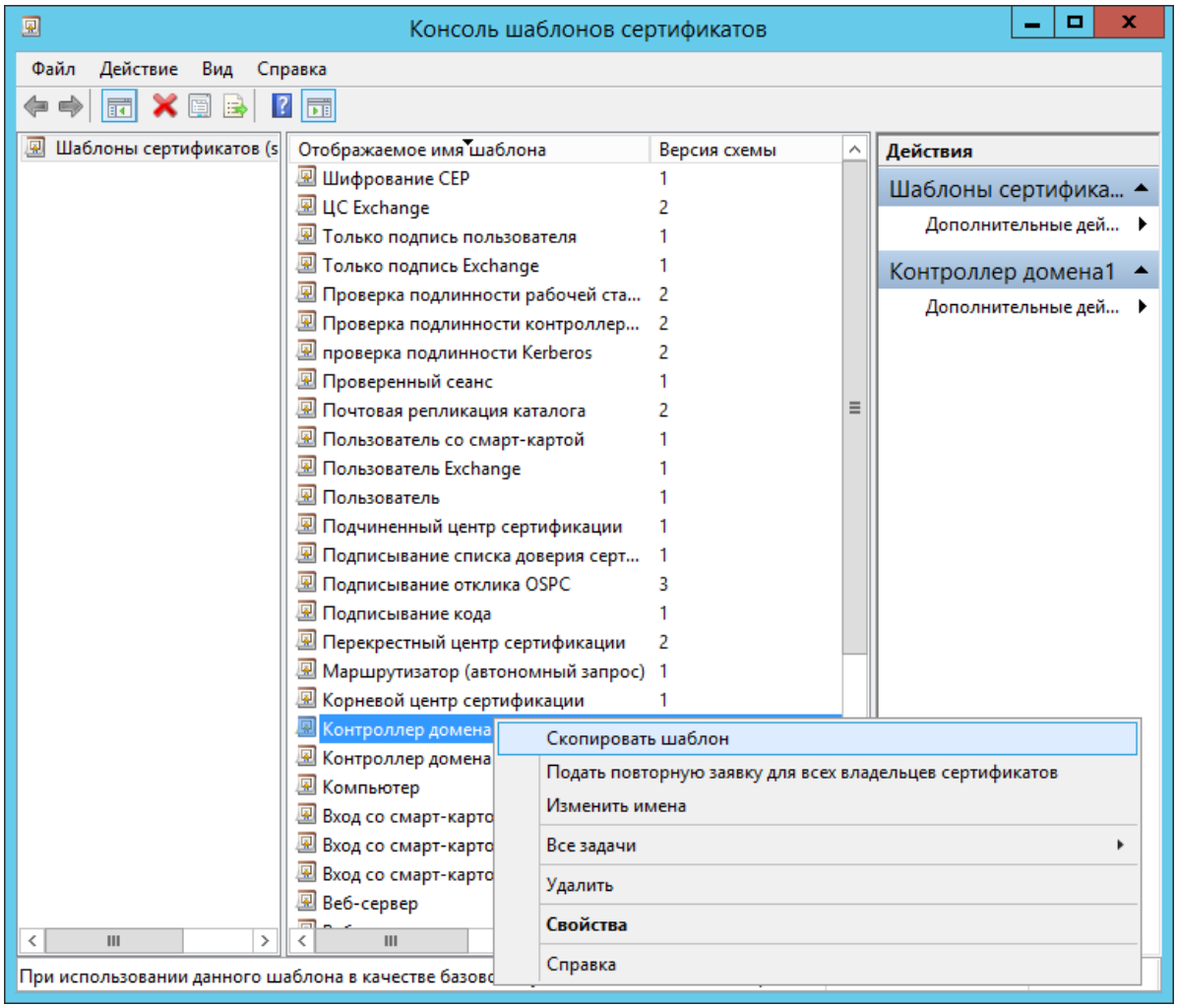
Если существующий шаблон не удовлетворяет требованию, к составу сертификата, необходимо его изменить. Для этого нужно создать копию шаблона, отредактировать её и включить в список шаблонов ЦС.

Откройте оснастку Центра сертификации (Пуск – Панель управления – Администрирование – Центр сертификации).

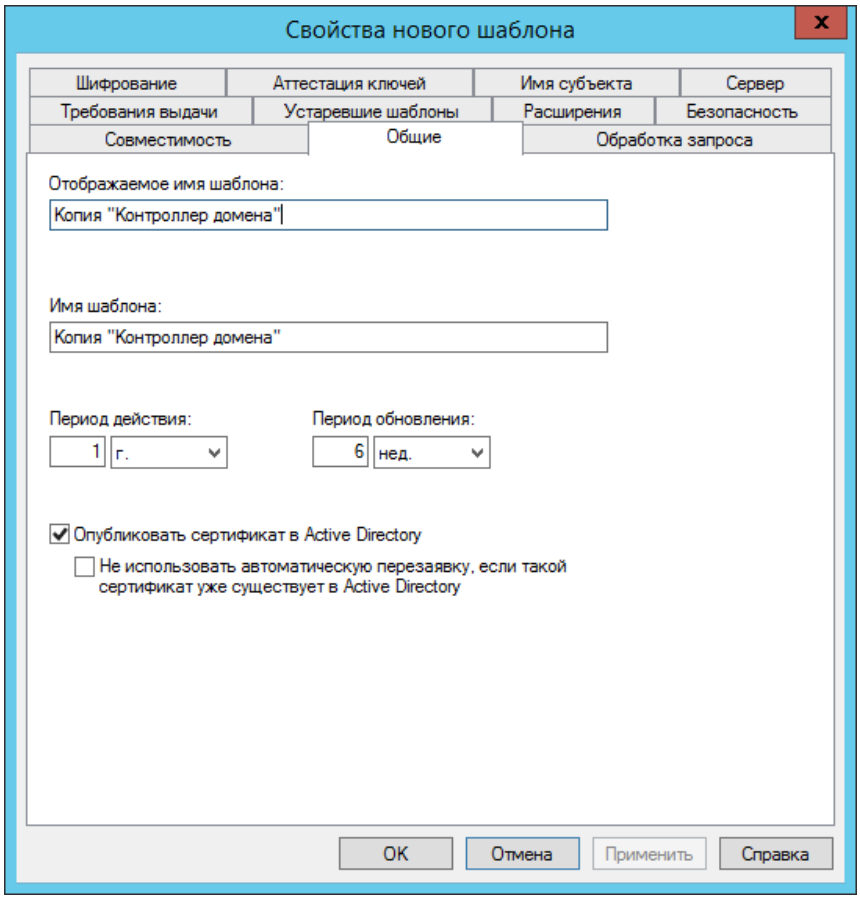
В оснастке выберите свой ЦС, откройте Шаблоны сертификатов.В контекстном меню нажмите Управление.



Запустится оснастка шаблонов сертификатов. В ней нужно выбрать редактируемый шаблон и нажать в контекстном меню «Скопировать шаблон».



Откроется форма, в которой можно изменить свойства шаблонов так, чтобы они соответствовали требованиям, описанным в п.п. Требования к сертификату контроллера домена, Требования к сертификату для входа по смарт-карте.



После сохранения нового шаблона нужно добавить его через список шаблонов способом, описанным в п. 6.2 Добавление шаблонов сертификатов на сервере.

6.3. 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** можно открыть оснастку mmc **Сертификаты,** затем в хранилище **Личное Локального компьютера** выбрать **Все задачи – Запросить новый сертификат**.

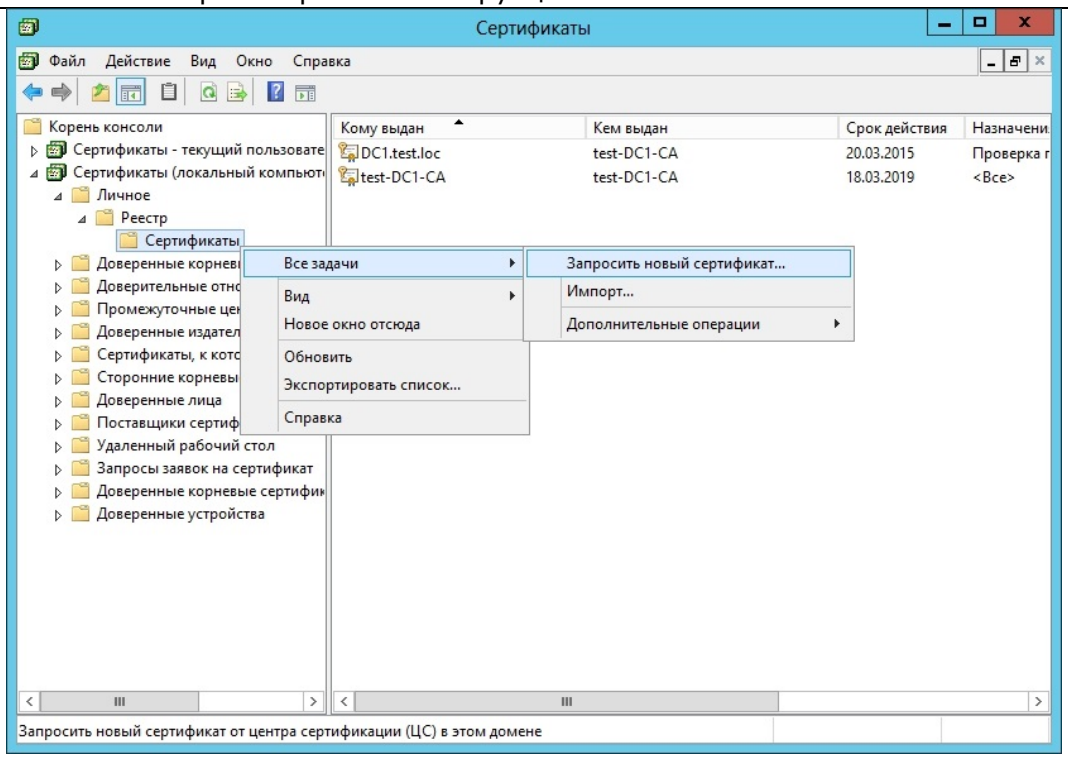


Рисунок 136. Запрос сертификата контроллера домена

Откроется мастер регистрации сертификатов. Нажмите **Далее**.

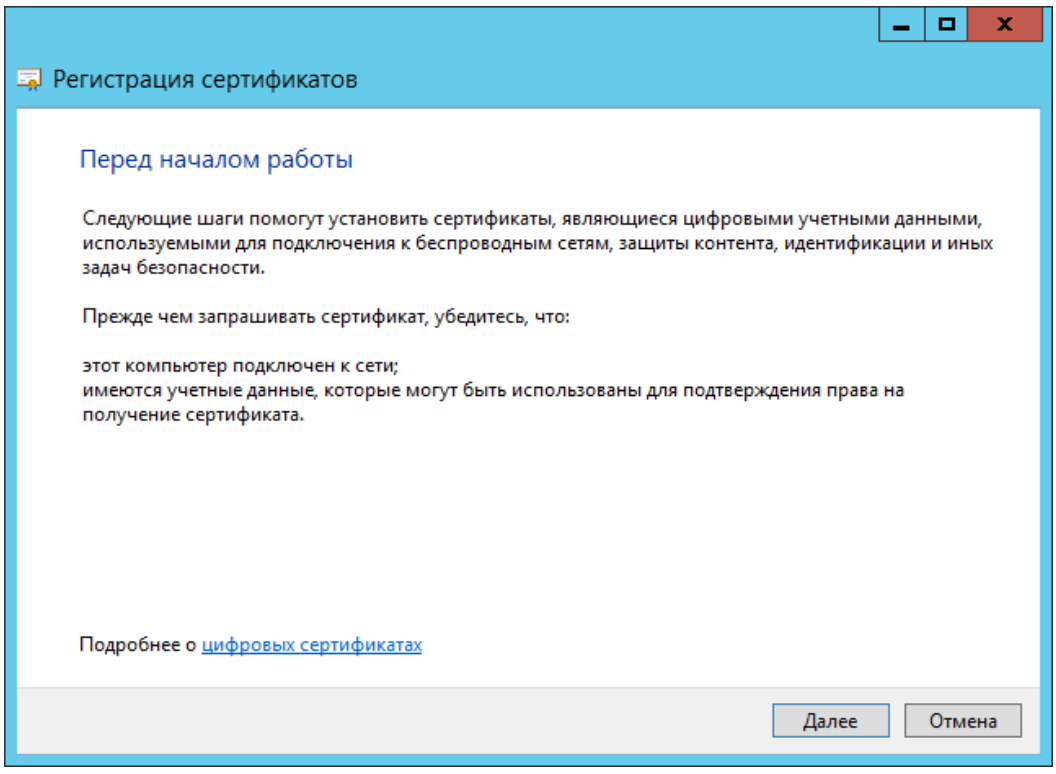


Рисунок 137. Мастер регистрации сертификатов

Откроется диалог выбора политики регистрации.

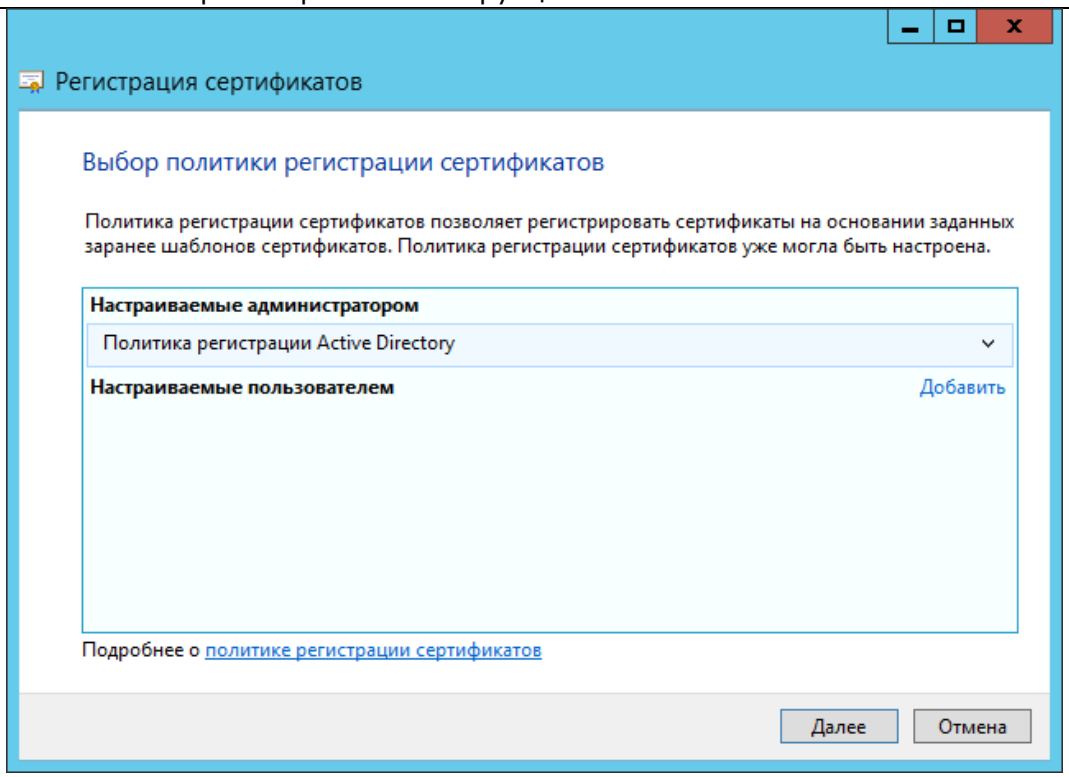


Рисунок 138. Выбор политики регистрации сертификатов

В данном окне нужно оставить параметры по умолчанию и перейти к следующему шагу, нажав **Далее**.

Из списка типов сертификатов выберите **Контроллер домена**.

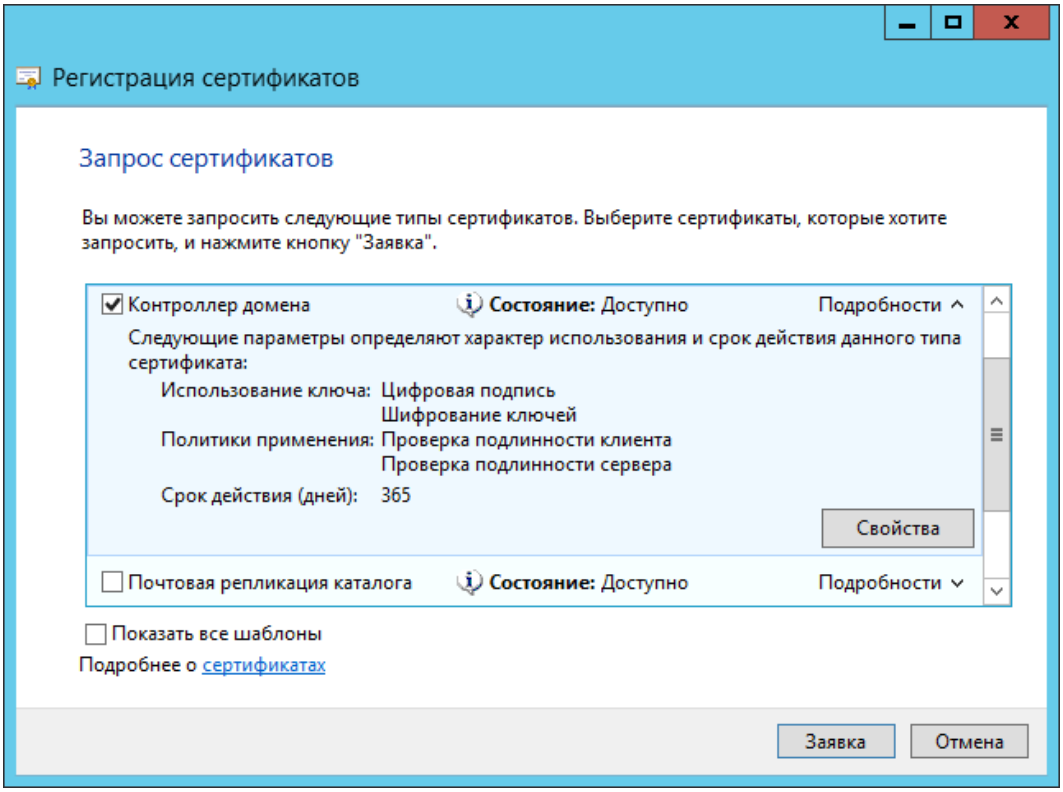


Рисунок 139. Запрос сертификата контроллера домена

Проверьте правильность и при необходимости выберите поставщика службы шифрования в **Свойствах** на вкладке **Закрытый ключ**.

Для того, чтобы выпустить сертификат на контроллер домена, нажмите кнопку **Заявка**. 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.

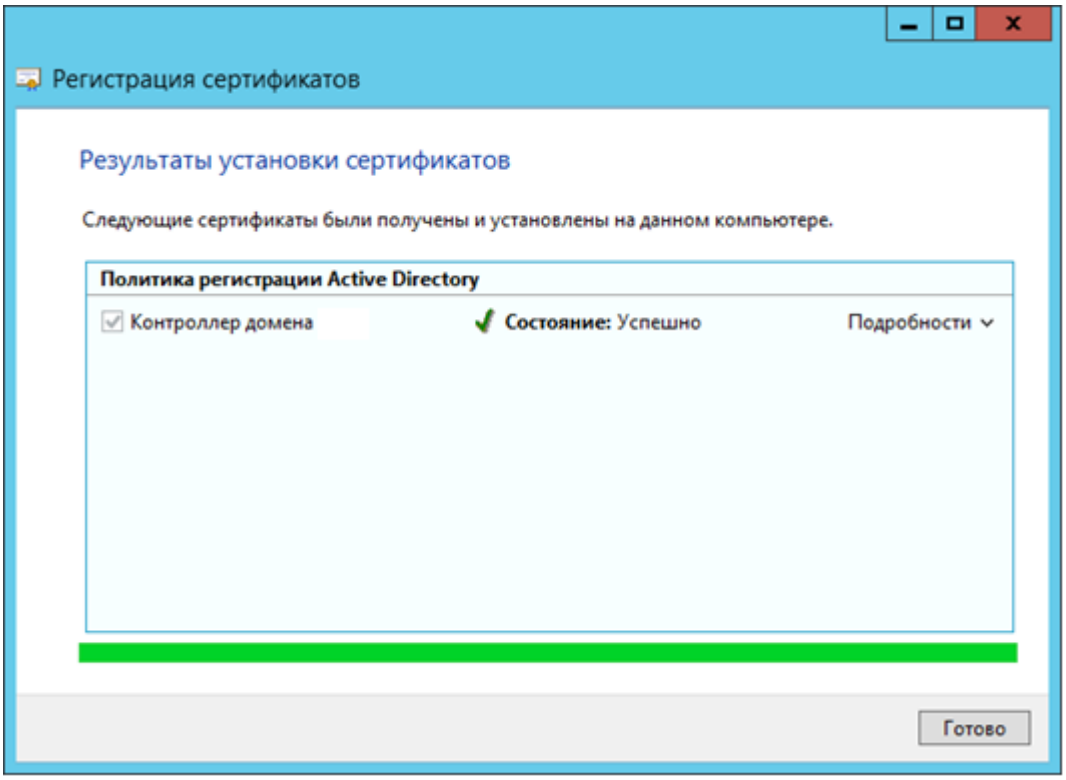


Рисунок 140. Результат установки сертификата контроллера домена

Развернув **Подробности** можно просмотреть сведения о сертификате.

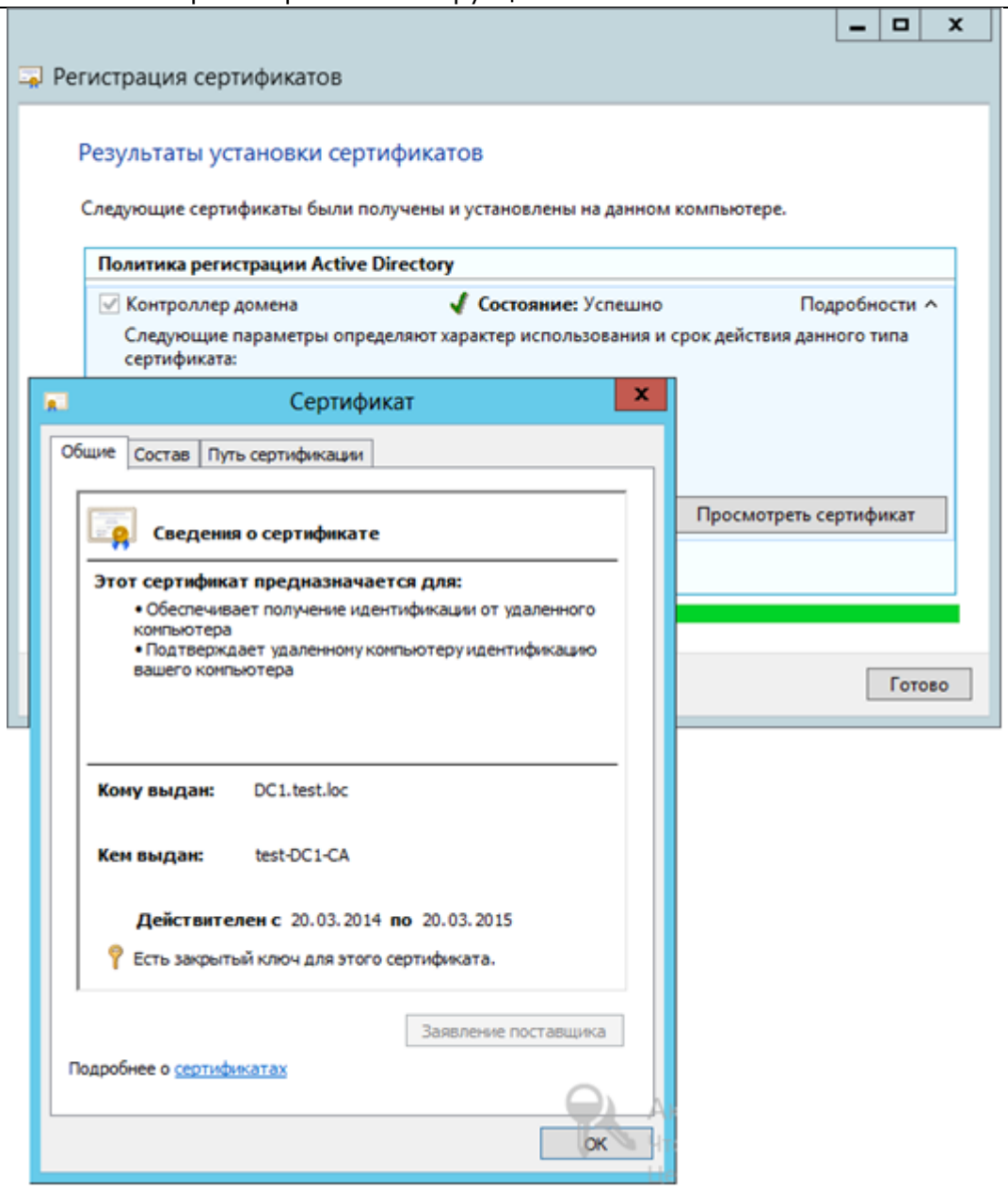


Рисунок 141. Просмотр сведений о сертификате

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

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

6.3.1. Требования к сертификату контроллера домена

- Сертификат должен иметь расширение точки распространения CRL, который указывает на действительный сертификат список отзыва (CRL), Например:

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

- При необходимости раздел субъекта сертификата должен содержать путь к каталогу серверного объекта (имя), например:

CN=Server1.northwindtraders.com OU = Domain Controller, DC = northwwindtraders, DC = com

- Раздел Использование должен содержать:

Цифровая подпись, Шифрование ключей

- Раздел Основные ограничения должен содержать:

[Тип темы = Конечный субъект, ограничения на длину пути = Отсутствует]

- Раздел расширенного использования ключа сертификата 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 дополнительное имя субъекта сертификата должен также содержать глобальный уникальный идентификатор (GUID) объекта 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»

6.4. 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 (ссылка на раздел в основной инструкции).

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**.

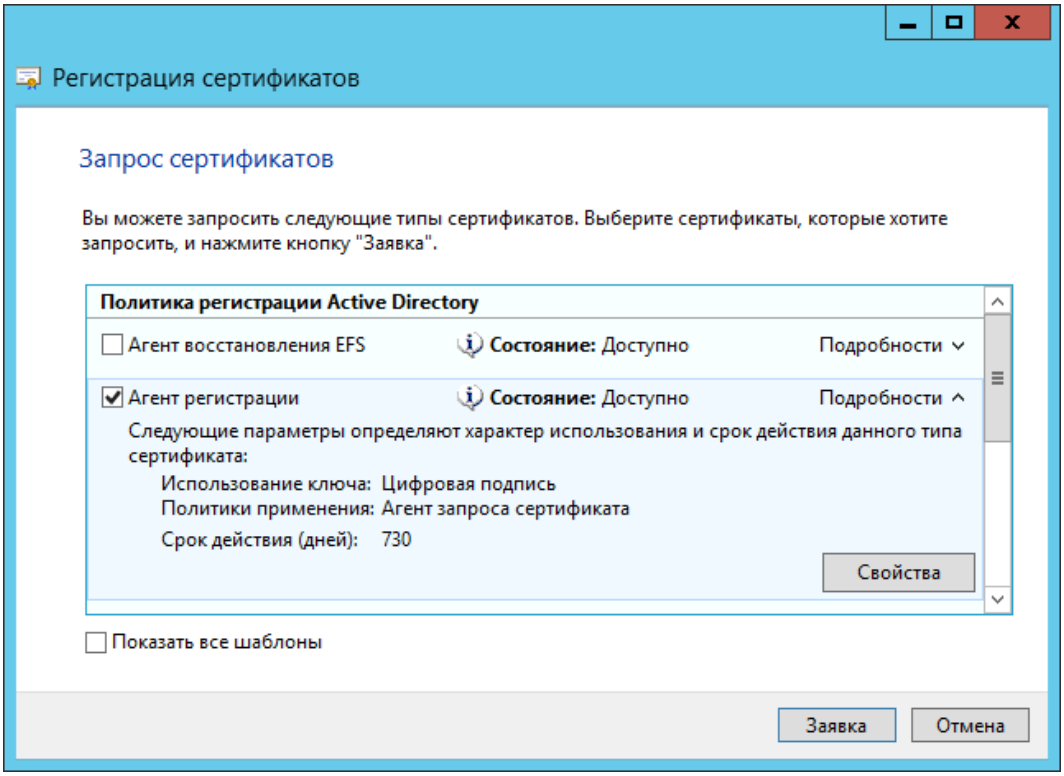


Рисунок 142. Выбор заявки Агента регистрации

Необходимо отредактировать шаблон сертификата, нажав на кнопку Свойства.

На вкладке Закрытый ключ в поле Поставщик службы шифрования нужно указать поставщика.

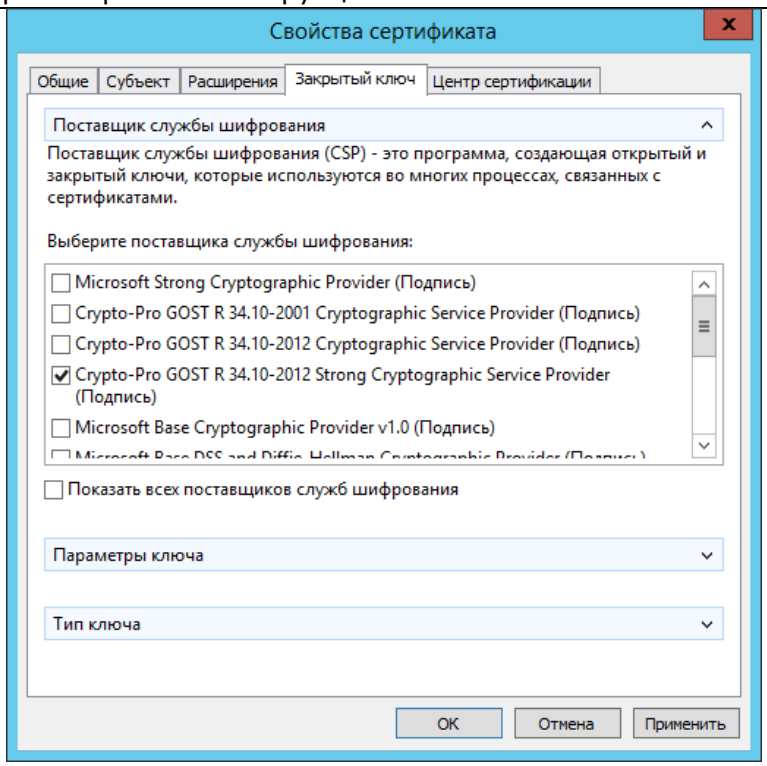


Рисунок 143. Выбор поставщика службы шифрования

На вкладке Центр сертификации обязательно должен быть указан соответствующий ЦС.

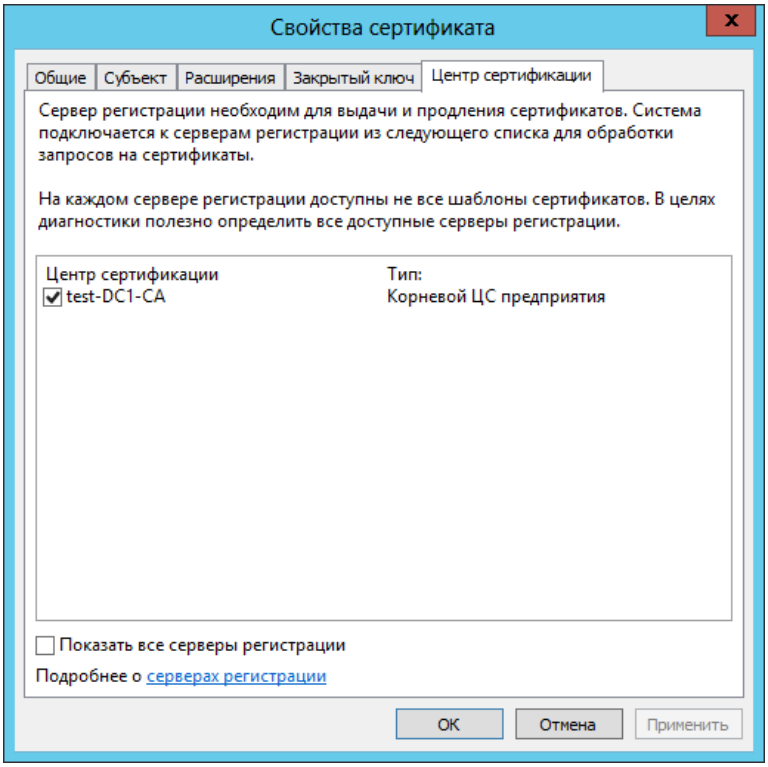


Рисунок 144. Выбор центра сертификации

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

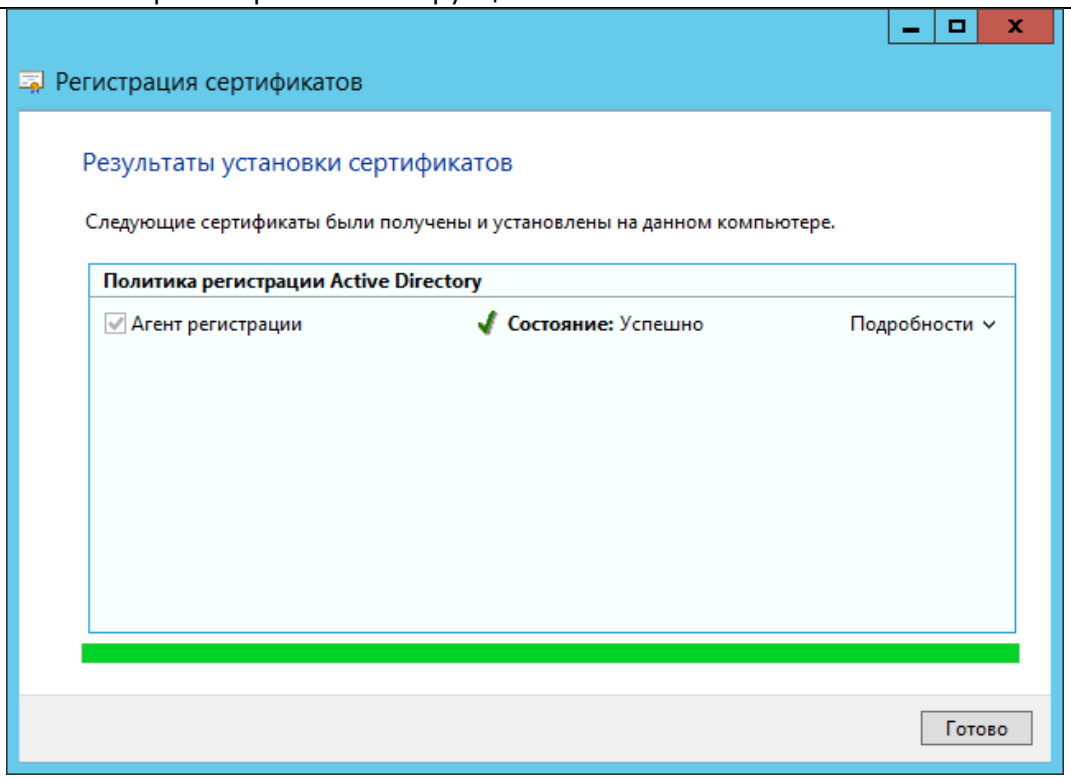


Рисунок 145. Результат выполнения установки сертификата Агента регистратора

6.5. 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 **Агента регистратора**, может выпускать сертификаты для других пользователей домена.

Для этого в оснастке **Сертификаты** нужно развернуть узел **Личные** и выбрать пункт **Сертификаты**, в котором выполнить **Все задачи – Дополнительные операции – Зарегистрироваться от имени.**

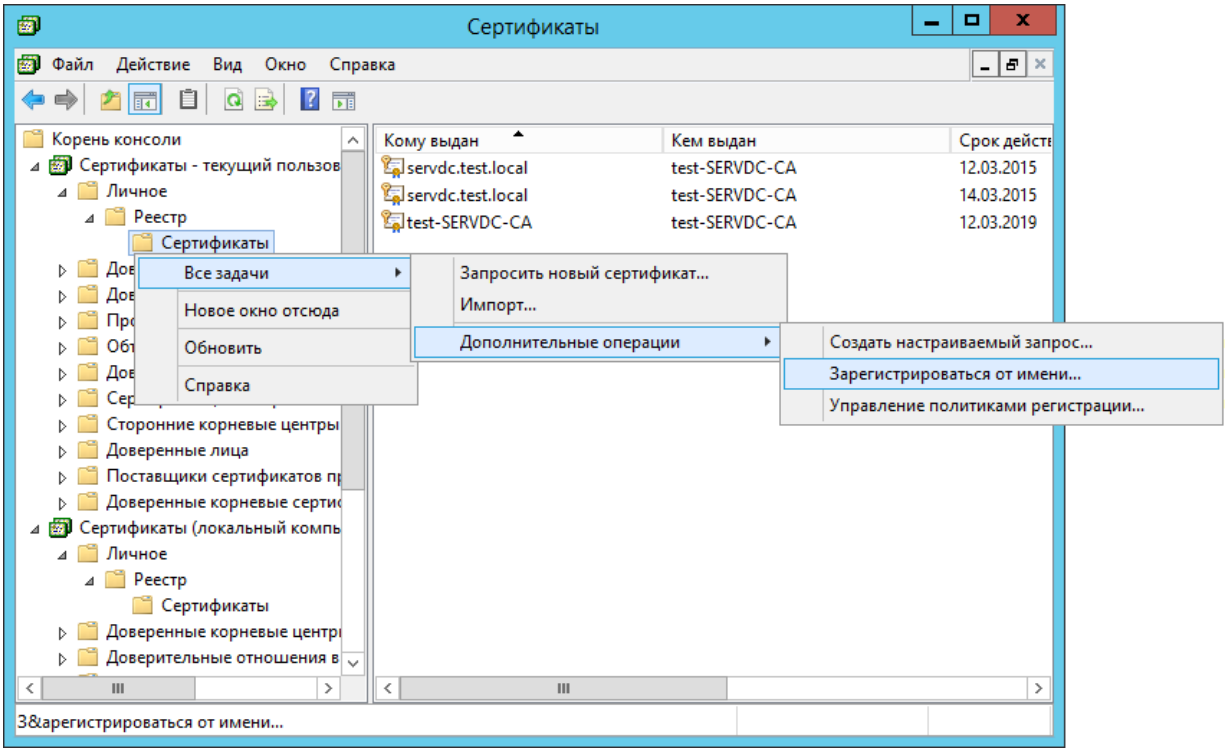


Рисунок 146. Выпуск сертификата пользователя смарт-карты

Перейдите к сертификату Агента регистрации, который будет использоваться для подписывания обрабатываемого запроса сертификата.

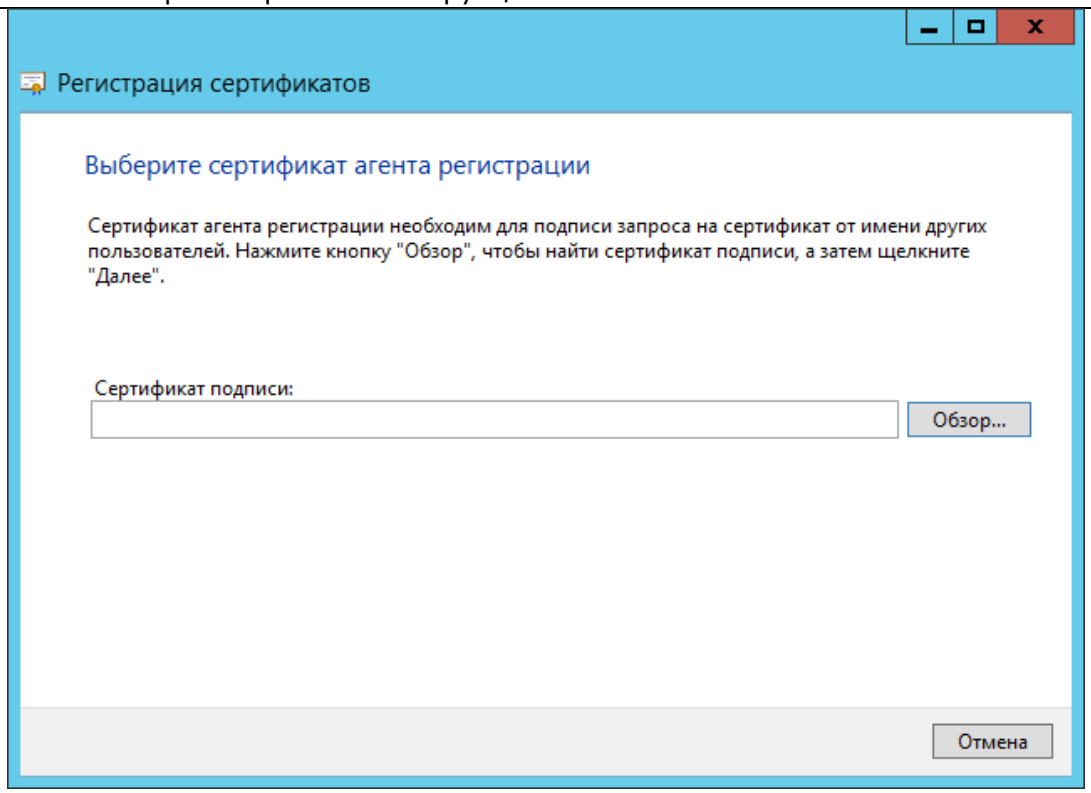


Рисунок 147. Выбор сертификата Агента регистрации

После выбора сертификата Агента регистрации из списка доступных сертификатов запрашивается пароль на доступ к этому сертификату.

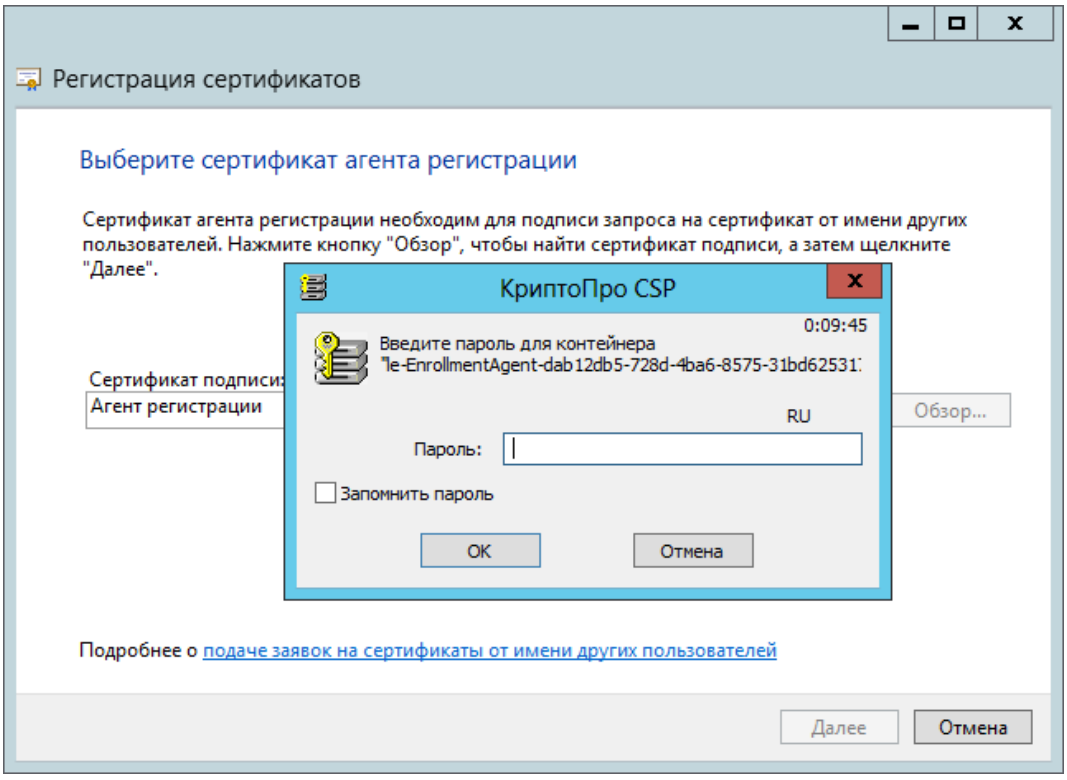


Рисунок 148. Ввод пароля для сертификата Агента регистрации

В мастере регистрации сертификатов указывается тип сертификата **Вход со смарт-картой**. Необходимо отредактировать параметры выпуска сертификата, для этого нажмите кнопку **Свойства**.

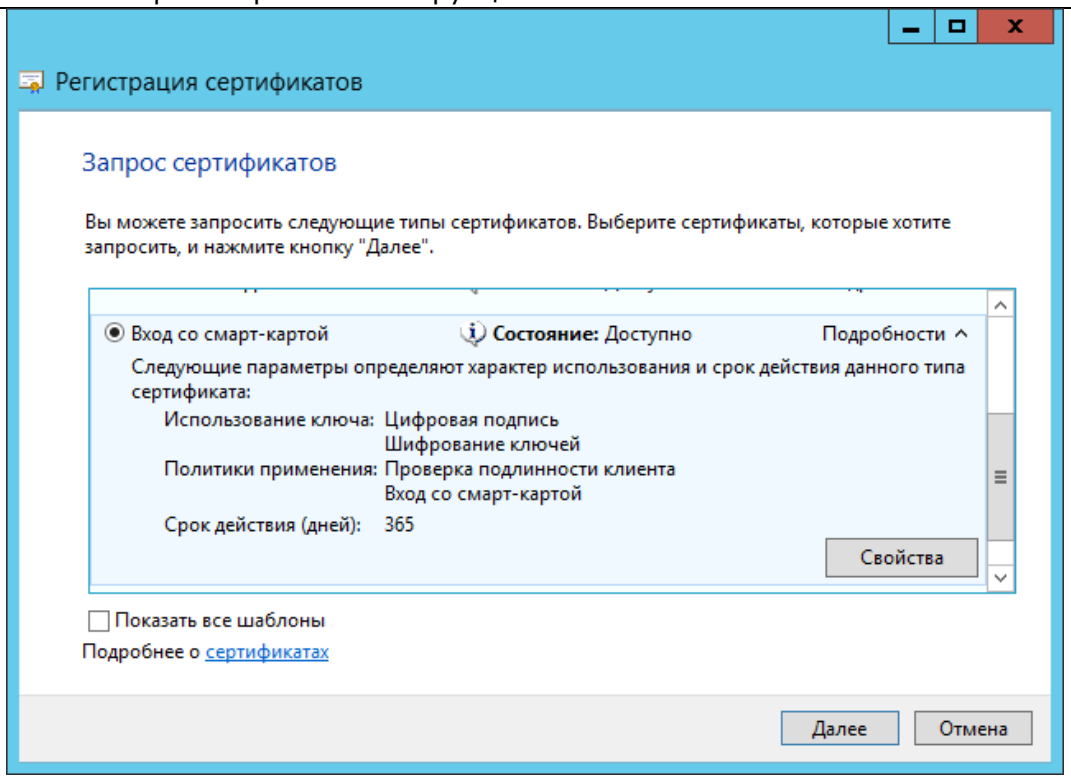


Рисунок 149. Выбор типа сертификата

Нужно указать поставщика службы шифрования и центр сертификации на соответствующих вкладках:

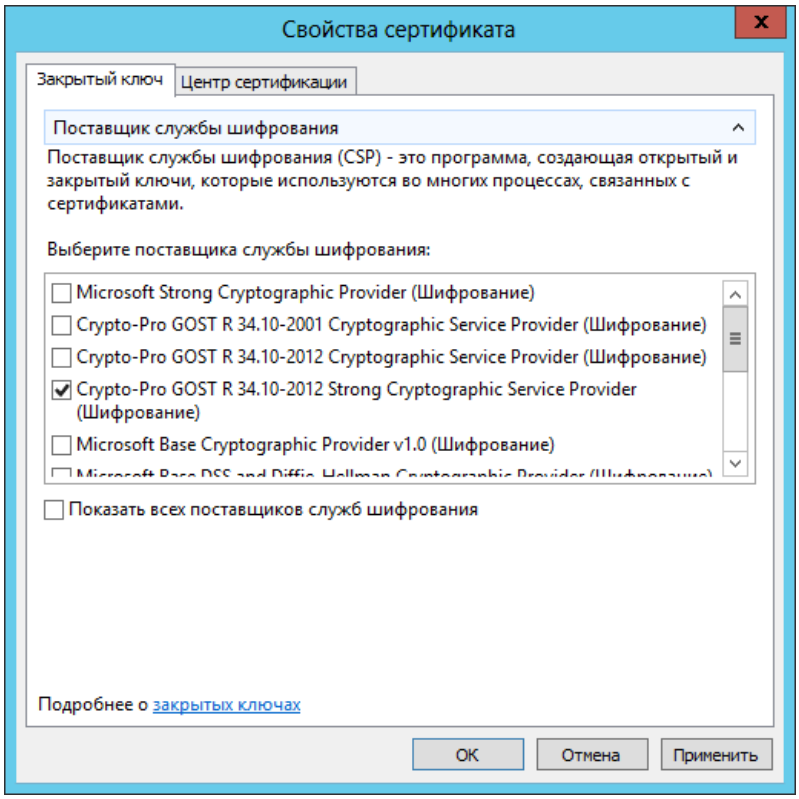


Рисунок 150. Выбор поставщика службы шифрования

Для сохранения выбранных параметров нужно нажать кнопку **Применить** и закрыть форму. В мастере создания сертификата нажмите **Далее**, чтобы перейти к следующему шагу и выбрать пользователя домена.

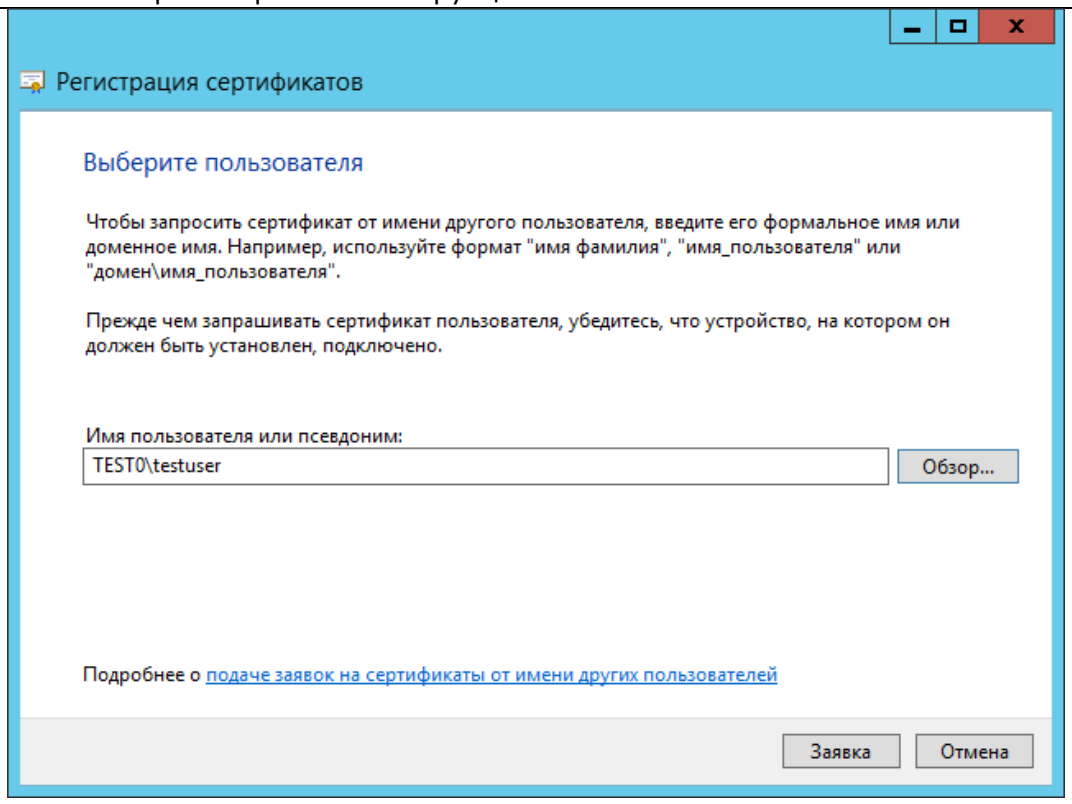


Рисунок 151. Выбор пользователя, для которого выпускается смарт-карта

Нажмите на кнопку **Заявка**, чтобы начать формирование контейнера и ключа.

Далее выбирается устройство для записи на носитель. 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.

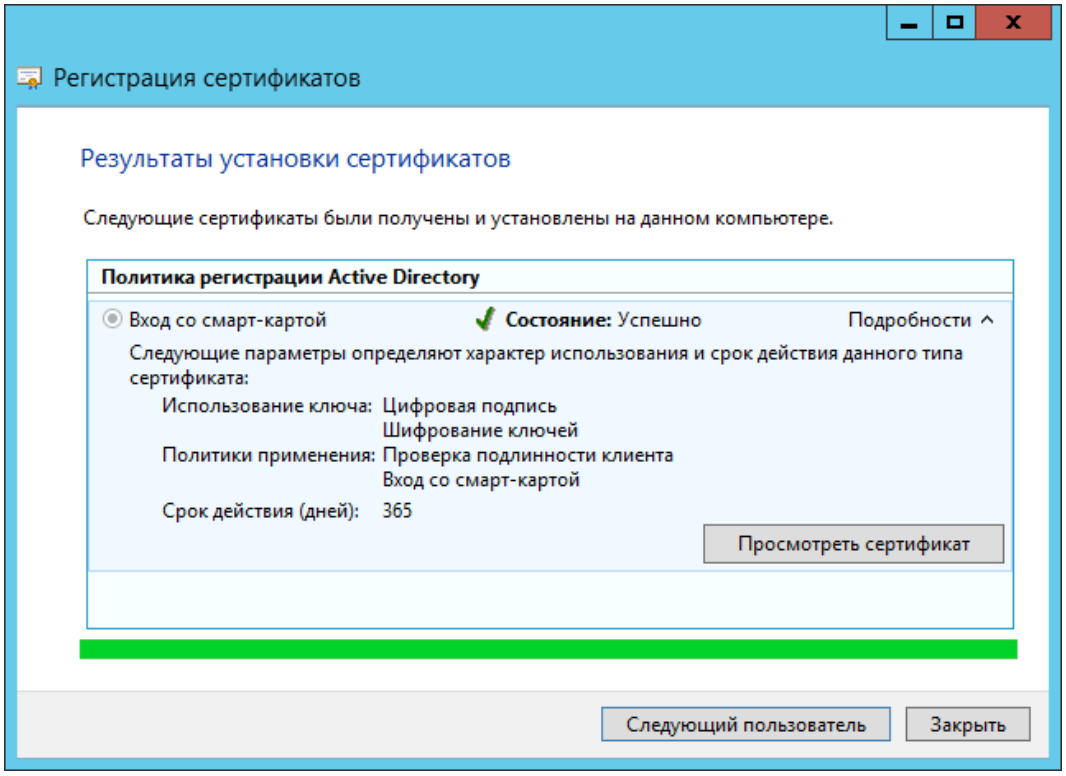


Рисунок 152. Результат выпуска сертификата

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

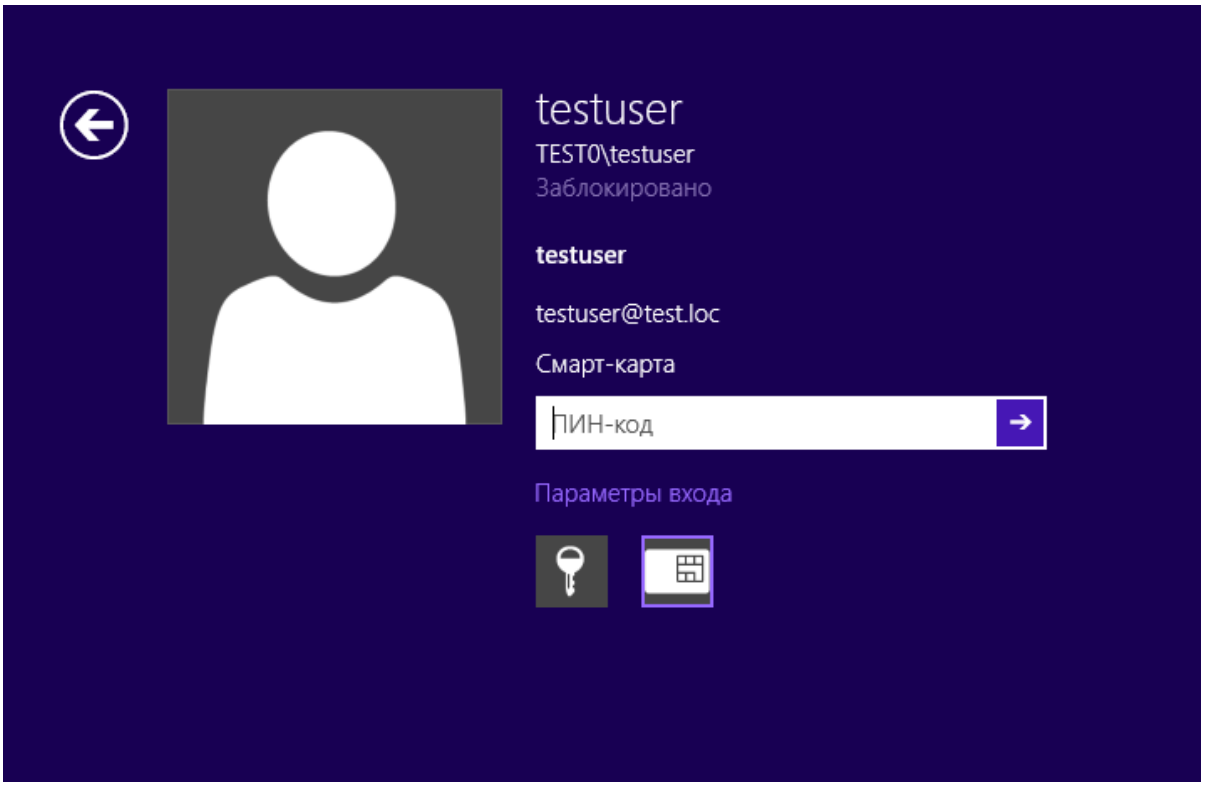


Рисунок 153. Авторизация с помощью смарт-карты пользователя домена

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.

6.5.1. Требования к сертификату для входа по смарт-карте

- Точка распространения CRL (где CRL - список отзыва сертификата) должна быть заполнена, доступна и находиться в оперативном режиме. Например:

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

- Использование ключа = Цифровая подпись
- Основные ограничения [Тип темы=Конечный субъект, Ограничения длины пути=нет] (Необязательно)
- Использование улучшенного ключа =

  Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
  (Проверка подлинности клиента (OID) 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)

- Дополнительное имя субъекта = другое имя: Основное имя пользователя= (UPN). Например:

основное имя пользователя = user1@name.com

UPN Другое имя OID: "1.3.6.1.4.1.311.20.2.3"

UPN Другое имя значение: Это должна быть ASN1-кодированная строка UTF8

- Тема = Различающееся имя пользователя. Это поле является обязательным дополнением, но заполнять его необязательно.

6.6. 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. И 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:

- Чтобы выполнить проверку подлинности пользователей в Active Directory, сторонние выпускающие центры сертификации должны находиться в хранилище NTAuth.
- Чтобы выполнять проверку 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.

6.6.1. Указания по настройке

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

6.6.1.1. 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.

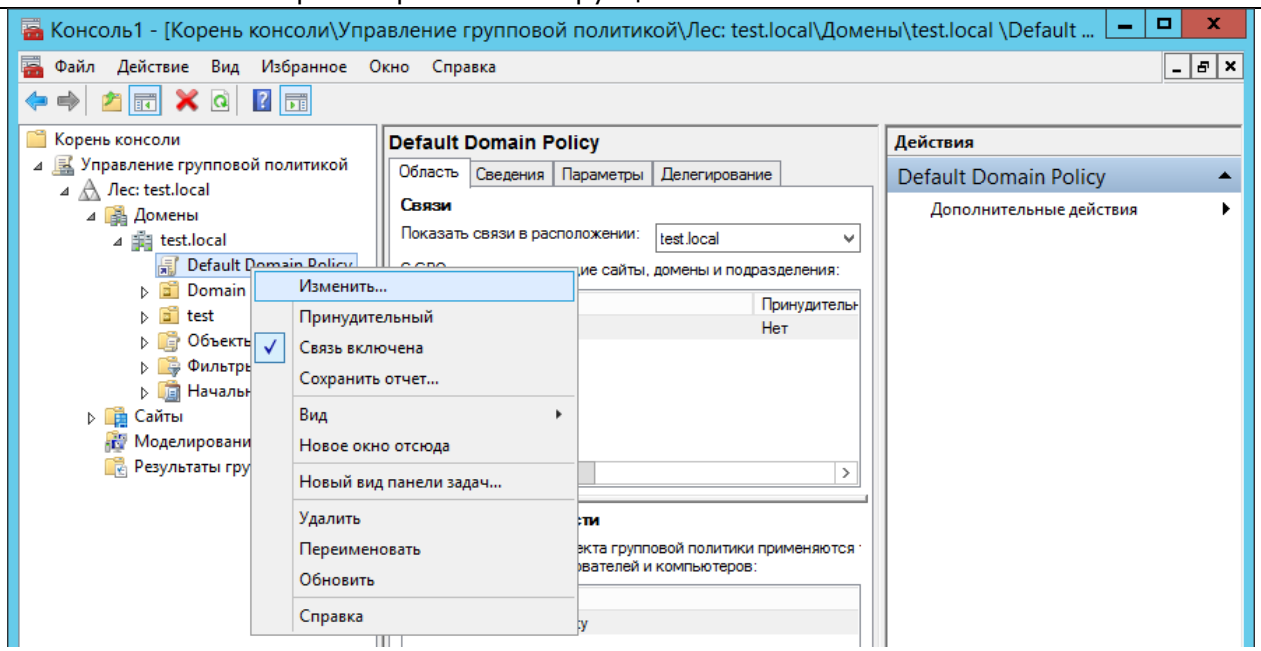


Рисунок 154. Оснастка Управление групповой политикой

Откроется окно Редактора управления групповыми политиками

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

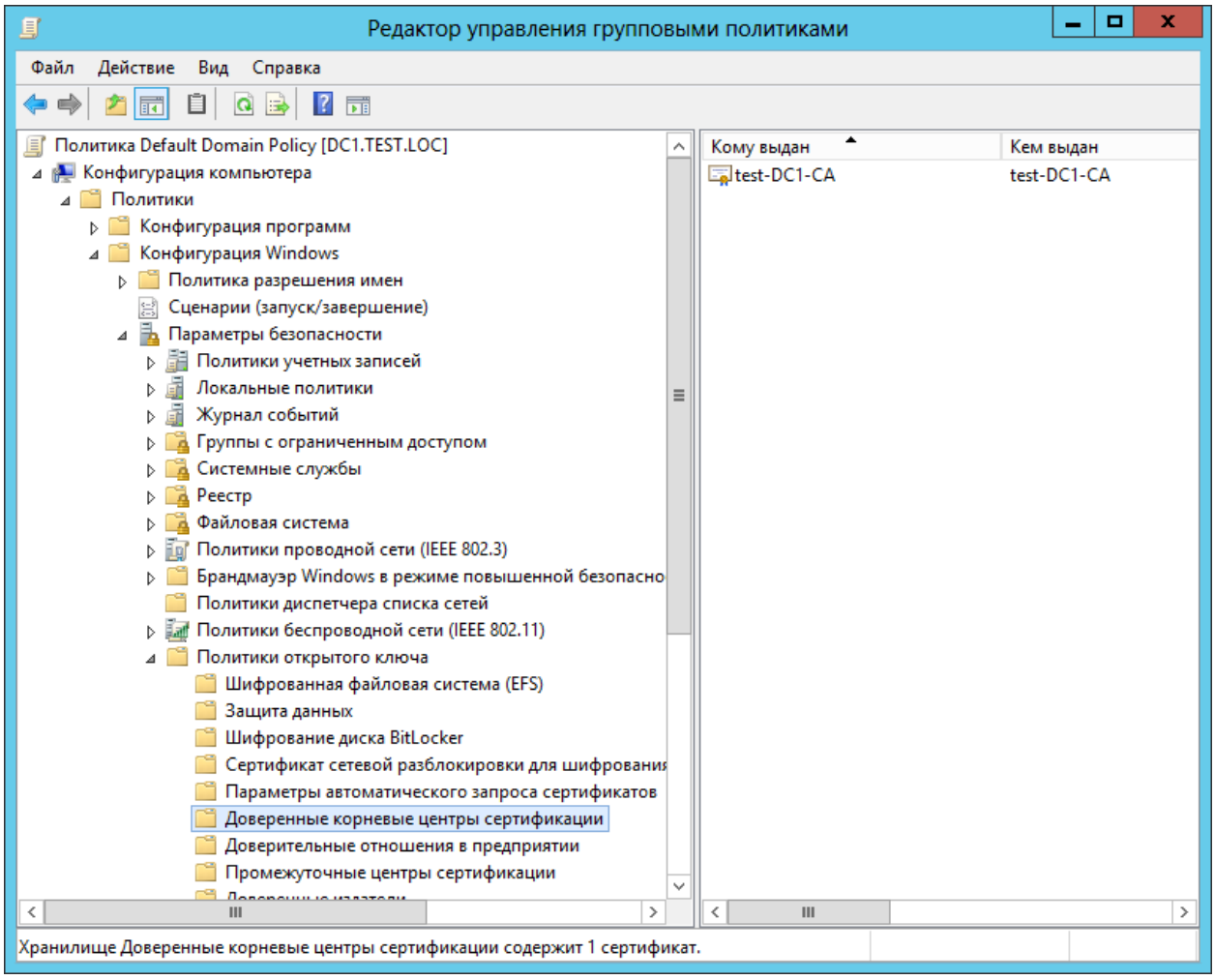


Рисунок 155. Добавление сертификата доверенного УЦ в групповые политики

6.6.1.2. 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=Public Key Services,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

Здесь <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

6.6.1.3. 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.

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

6.6.2. Вход в домен по УЭК

В КриптоПро Winlogon реализована возможность использования УЭК для авторизации в домене. Для того, чтобы настроить эту функцию, нужно выполнить на сервере AD следующие действия:

1. Включить в настройках групповой политики AD параметр, разрешающий при входе выбор из сертификатов, содержащих электронную подпись.

Параметр **Разрешить ключи подписей для входа** включается в редакторе групповых политик (gpedit.msc) на контроллере домена в узле **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Смарт-карта**.

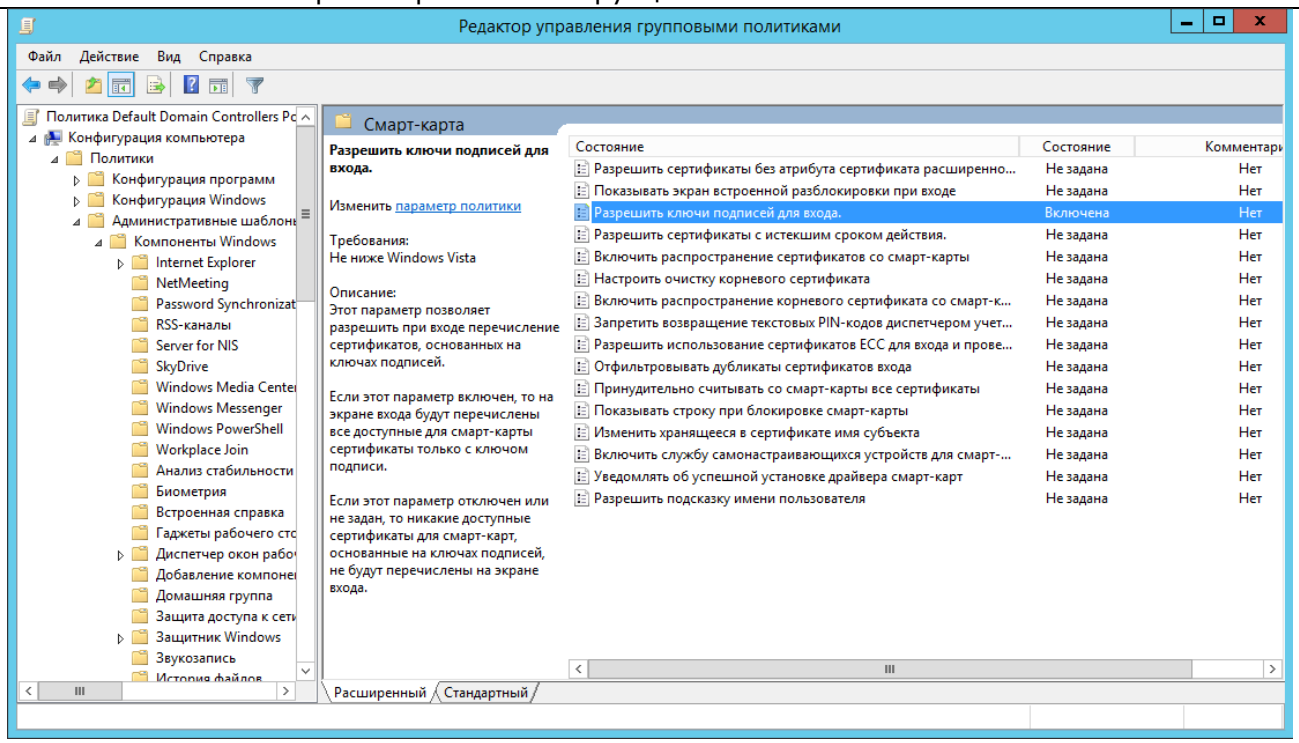


Рисунок 156. Разрешение входа в домен по ключам подписей

2. Обеспечить доверие ко всей цепочке сертификатов на сервере и распространить его с помощью групповой политики (см. п.п. 6.6.1.1 и 6.6.1.2)
3. Обеспечить доступ к списку отзыва сертификатов (CRL).

На ЦС, выпускающем сертификат для УЭК должен быть использован шаблон с именем «Вход со смарт-картой». Выпуск сертификата подробно описан в п.п. 6.2 и 6.5.

На клиентской машине необходимо:

1. Установить СКЗИ КриптоПро УЭК CSP.
2. Обеспечить взаимодействие с CV-сервисом по 443 порту.

Для проверки доступности CV-сервиса откройте утилиту настройки УЭК (**Пуск ⇒ Программы ⇒ КриптоПро ⇒ UEC tool**), введите адрес сервера, на котором расположен сервис, нажмите кнопку «Тест».

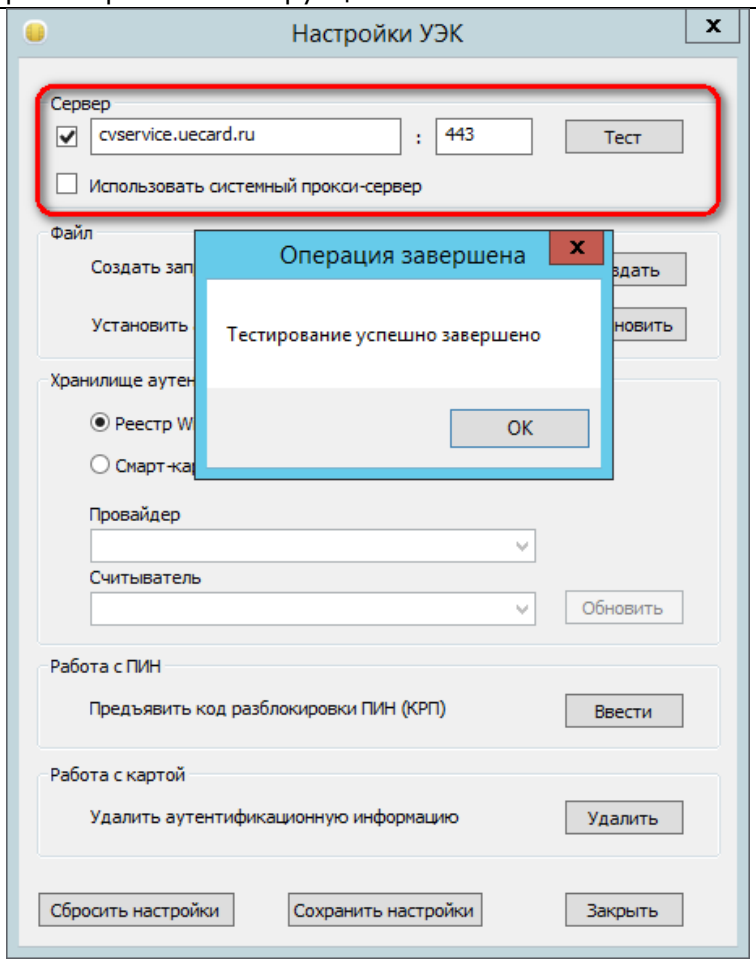


Рисунок 157. Проверка доступности CV-сервиса

3. Через панель управления СКЗИ КриптоПро УЭК CSP нужно указать в свойствах носителя, что он зарегистрирован в Smartcard Winlogon.

Для этого откройте панель управления (**Пуск ⇒ Программы ⇒ КриптоПро ⇒ КриптоПро УЭК CSP**), на вкладке **Оборудование** нажмите **«Настроить типы носителей...»** Выберите из предложенного списка тип носителя, соответствующий используемой УЭК и откройте свойства носителя. На вкладке **Свойства карты** должен быть проставлен флажок **«Зарегистрирован в smartcard winlogon»**.

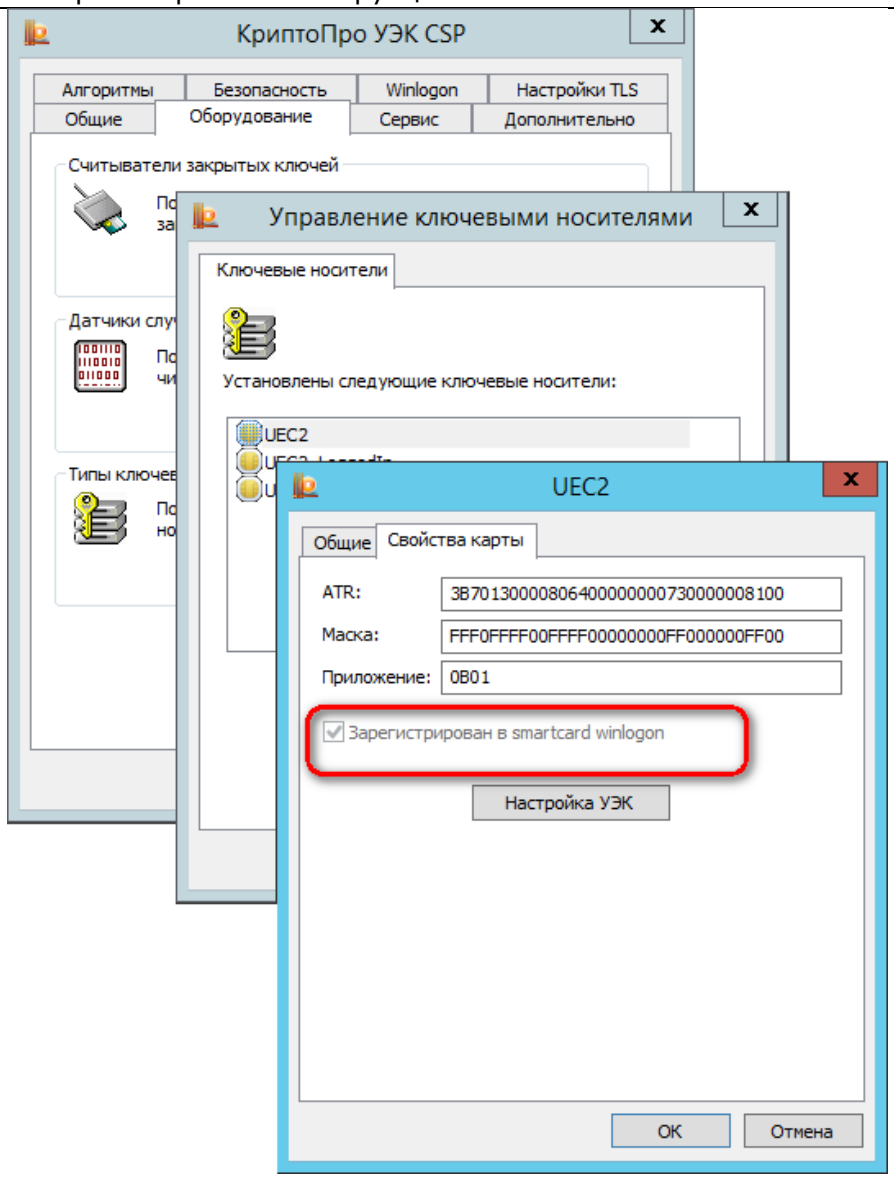


Рисунок 158. Настройка параметров ключевого носителя

Если флажок не проставлен, то нужно удалить ключевой носитель в форме **Управление ключевыми носителями**, добавить его заново и проставить этот параметр при добавлении.

4. Подключить к компьютеру пользователя считыватель смарт-карт, соответствующий спецификации для доступа к смарт-картам PC/SC (при необходимости установить драйвер считывателя вручную).

После включения всех вышеперечисленных настроек нужно убедиться, что групповая политика применена к клиентским учетным записям и компьютерам, и авторизоваться в домене с помощью УЭК.

7. Использование КриптоПро CSP при работе с почтовым клиентом The Bat!

Для того, чтобы использовать защиту 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.

7.1. Настройка параметров S/MIME почтового клиента

1. В главном меню The Bat! выберите **Свойства – S/MIME и TLS…**
2. В окне **Параметры S/MIME и TLS** укажите следующие настройки:
   - в блоке **Реализация S/MIME и сертификаты TLS** выберите Microsoft CryptoAPI;
   - флаг **Всегда шифровать отправителю** ставится, если необходимо, чтобы исходящая почта шифровалась с помощью сертификата получателя в случае, если такой сертификат есть;
   - **Криптопровайдер** – выберите из выпадающего списка поставщика служб шифрования;
   - флаг **Никогда не использовать других криптопровайдеров** ставится, если данный почтовый клиент не планируется использовать с другими поставщиками служб шифрования;
   - **Алгоритм шифрования** – указывается алгоритм шифрования, соответствующий выбранному криптопровайдеру;
   - **Хэш-алгоритм подписи** – указывается хэш-алгоритм подписи;
   - **Помнить связи e-mail адресов с сертификатами для подписи** ставится для автоматического выбора сертификатов;
   - **Помнить связи e-mail адресов с сертификатами для шифрования** ставится для автоматического выбора сертификатов.

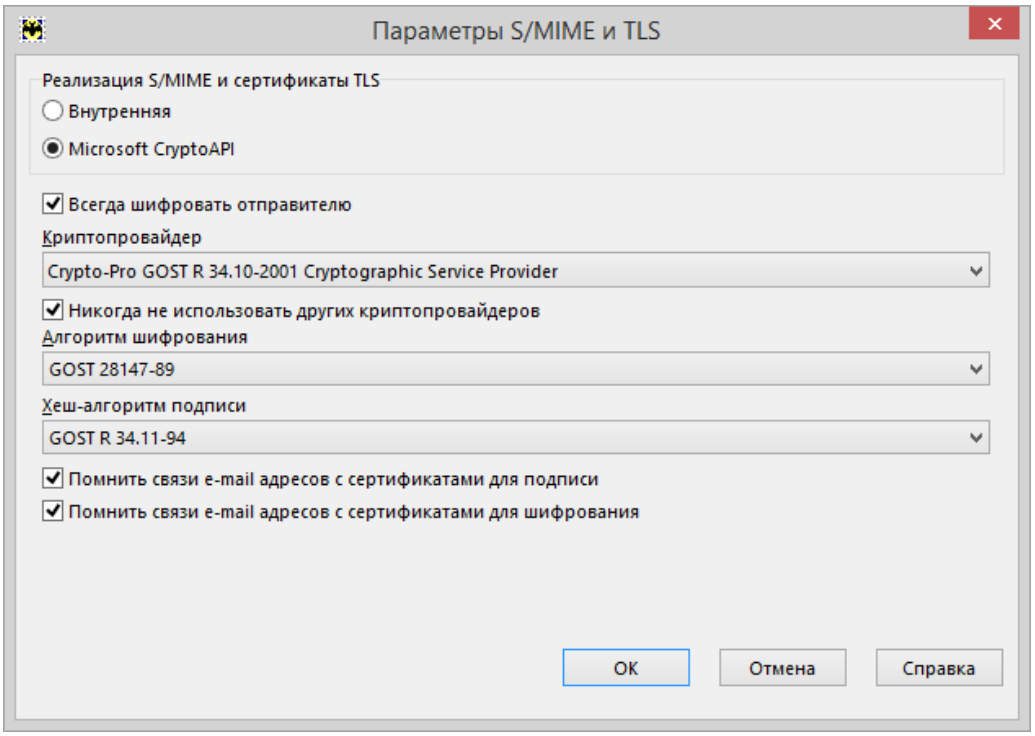


Рисунок 159. Настройка параметров S/MIME и TLS

3. Сохраните настройки, нажав кнопку **ОК**.

7.2. Настройка почтового ящика

1. Для изменения параметров почтового ящика выделите почтовый ящик и в главном меню The Bat! выберите **Ящик – Свойства почтового ящика…**
2. В окне **Свойства почтового ящика** выберите раздел **Параметры**. В блоке «Редактор писем» должно быть отмечено флажком поле **Авто-S/MIME**. Также можно включить опции **Подписать перед отправкой** и **Зашифровать перед отправкой**.

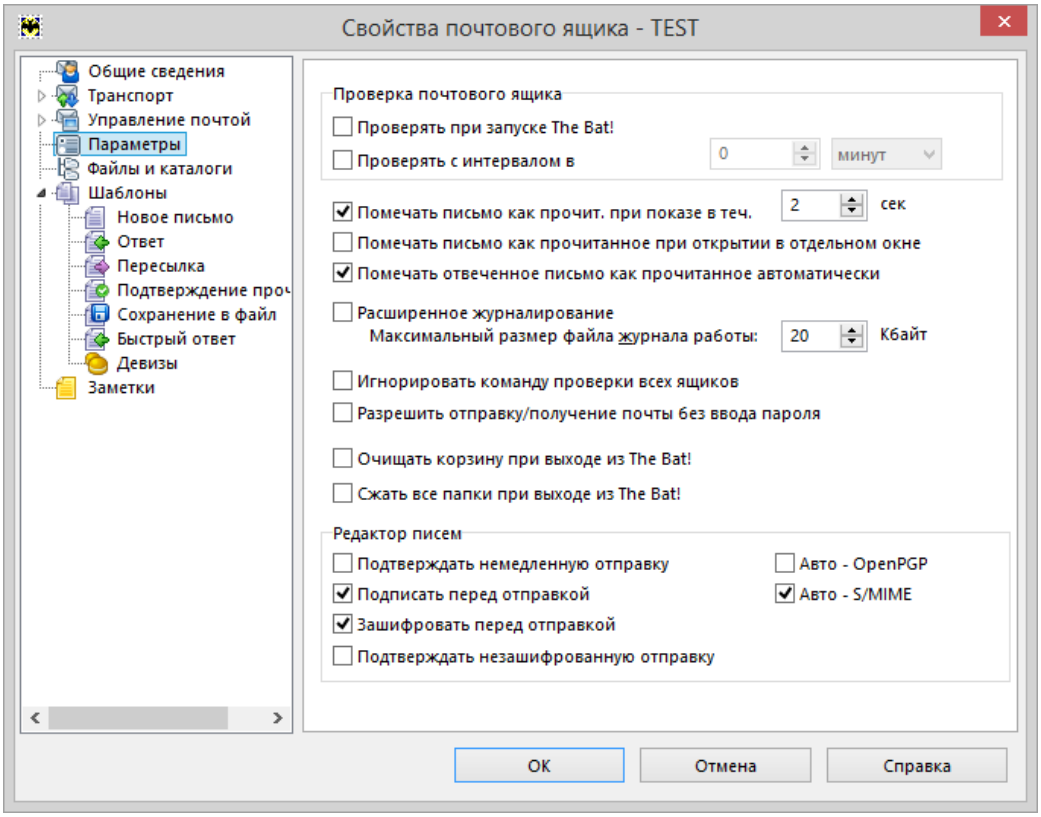


Рисунок 160. Редактирование свойств почтового ящика

3. Сохраните настройки, нажав кнопку **ОК**.

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

7.3. 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 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.

1. При просмотре письма нужно нажать кнопку **Просмотреть действительную подпись**.

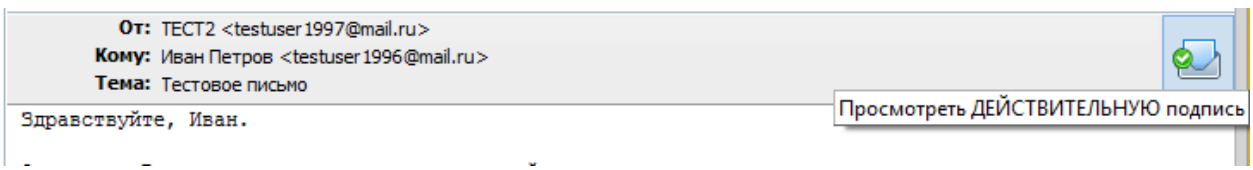


Рисунок 161. Функция просмотра подписи в The Bat!

2. В окне проверки подписи нажмите **Просмотреть свойства сертификата**.

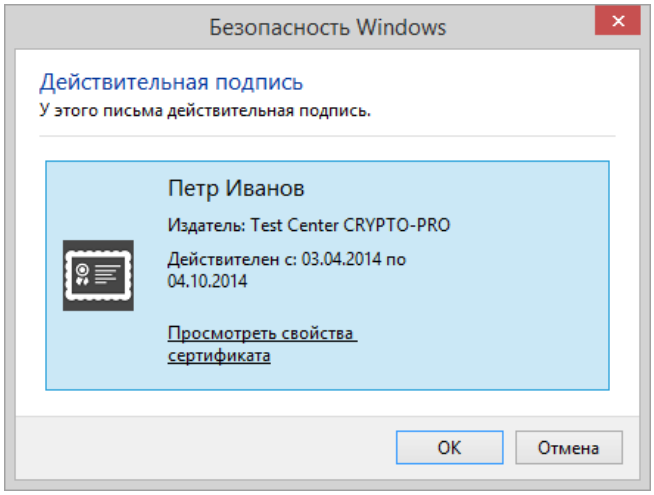


Рисунок 162. Форма просмотра подписи

3. В окне просмотра свойств сертификата нажмите **Установить сертификат**.

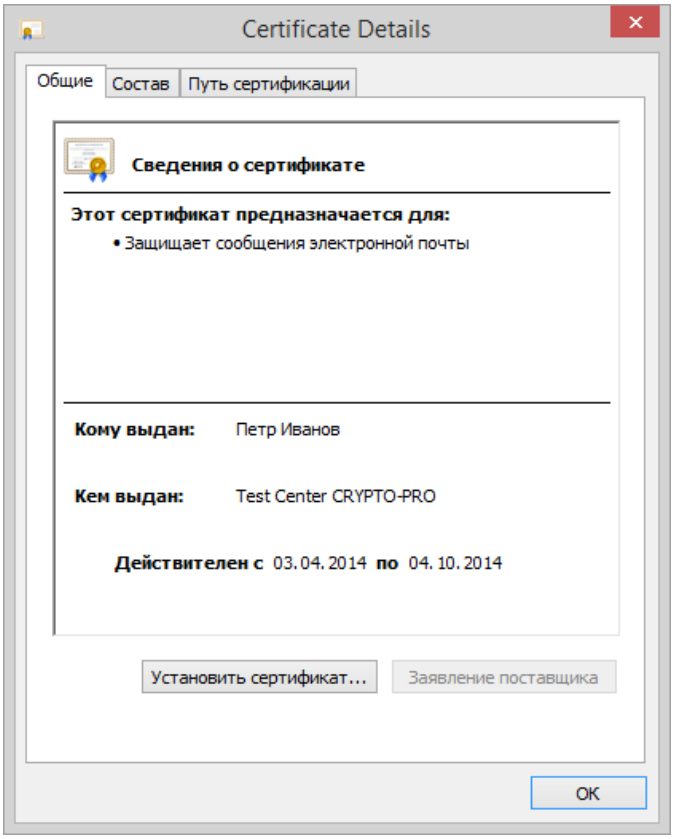


Рисунок 163. Форма просмотра сертификата

4. В открывшемся мастере импорта сертификатов выберите хранилище Текущего пользователя и нажмите **Далее**.

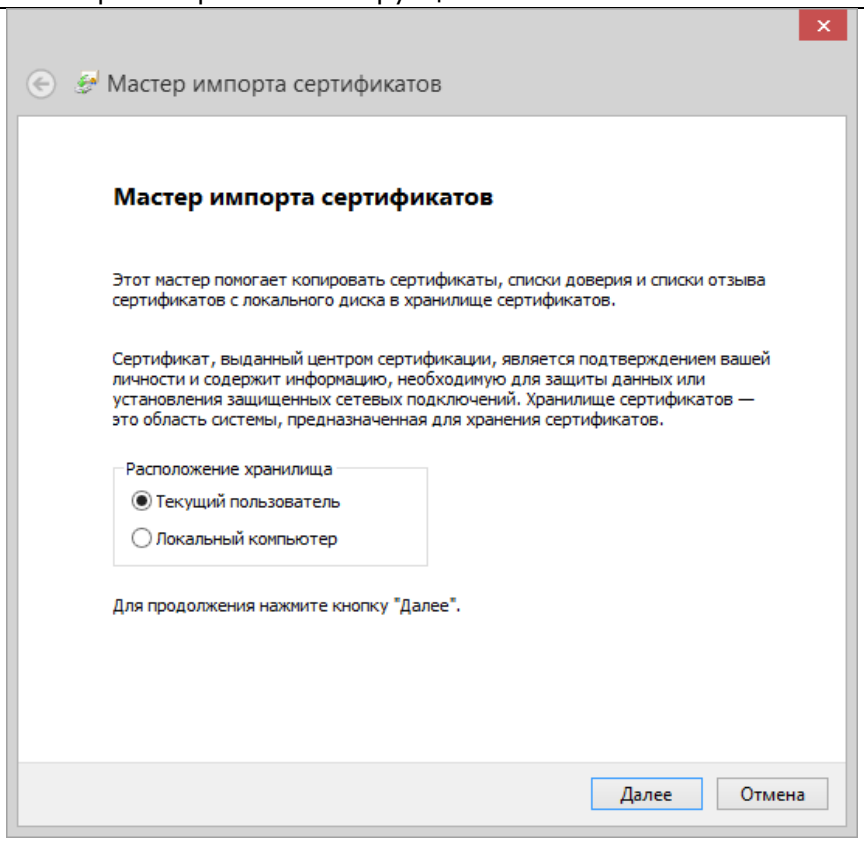


Рисунок 164. Выбор расположения хранилища при импорте сертификата

5. На следующем шаге вручную выберите хранилище **Другие пользователи** и нажмите **Далее**.

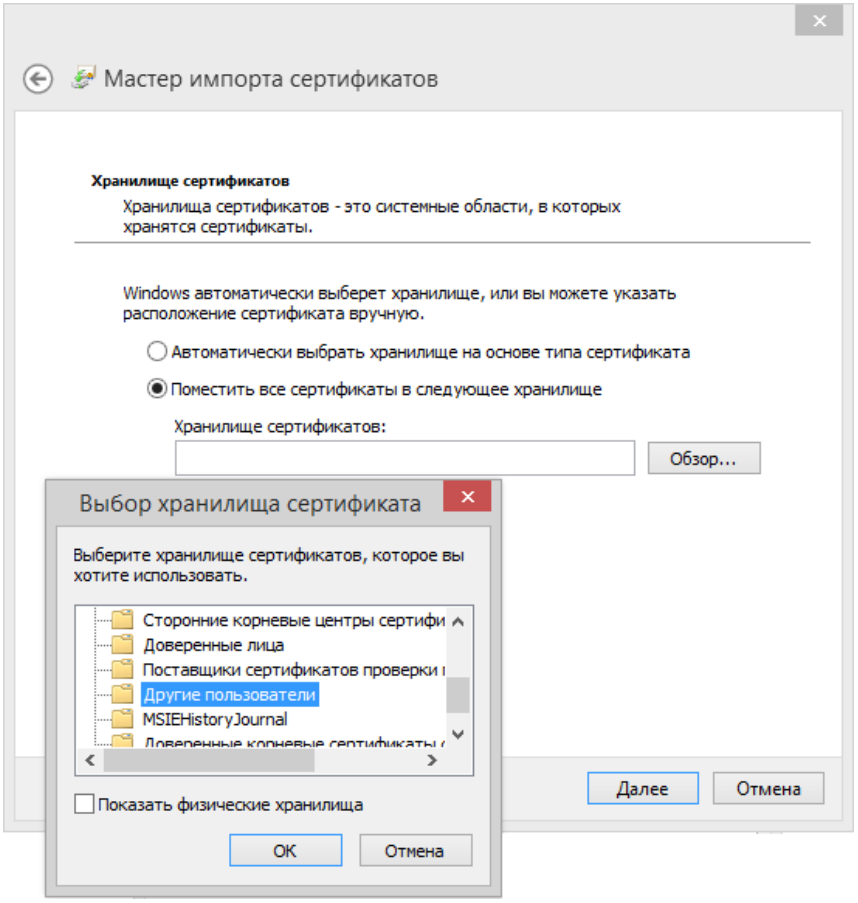


Рисунок 165. Выбор хранилища при импорте сертификата

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

После этого в адрес владельца сертификата можно отправлять зашифрованные письма, воспользовавшись кнопкой **Зашифровать перед отправкой** в окне редактирования письма.

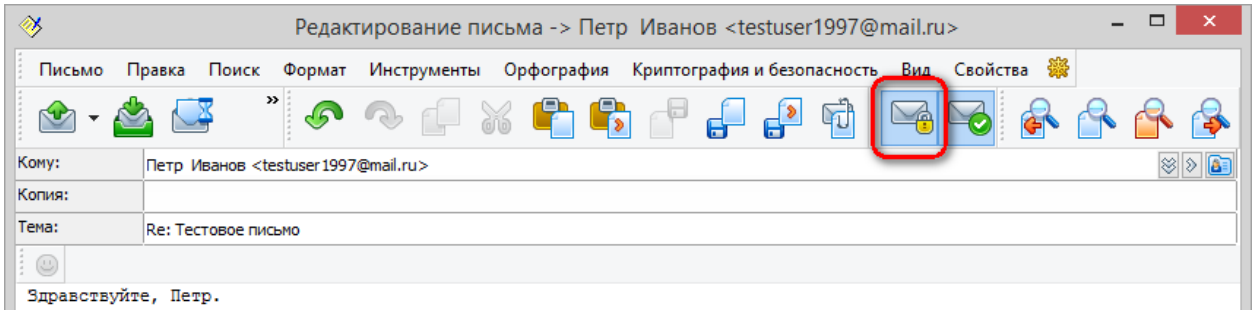


Рисунок 166. Функция шифрования в форме редактирования письма

При этом перед отправкой предлагается сначала выбрать сертификат для шифрования письма (его можно выбрать из списка доступных или он выбирается автоматически, по е-мейлу получателя письма), а потом ввести пароль для контейнера личного сертификата, с помощью которого будет подписано письмо, если Вы указали **Подписать перед отправкой**.

8. Использование КриптоПро CSP при работе с почтовым клиентом Outlook 2013

Использование средств криптографической защиты в Outlook 2013 во многом совпадает с использованием в Outlook ранних версий.

8.1. Конфигурация Outlook 2013

Выберите пункт **Параметры** (**Options**) меню **Файл** (**File**).

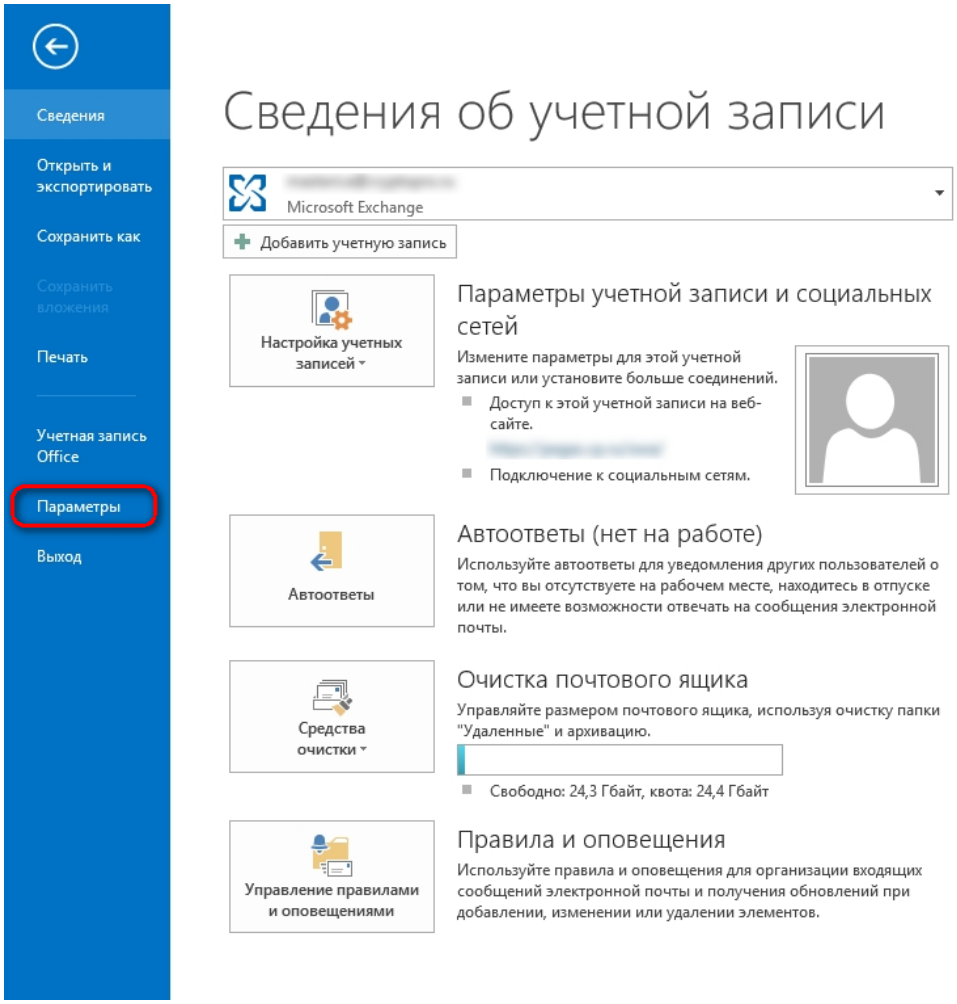


Рисунок 167. Меню Файл Outlook

В открывшемся окне выберите в закладке **Центр управления безопасностью** (**Trust Center**) пункт **Параметры Центра управления безопасностью** (**Trust Center Settings**).

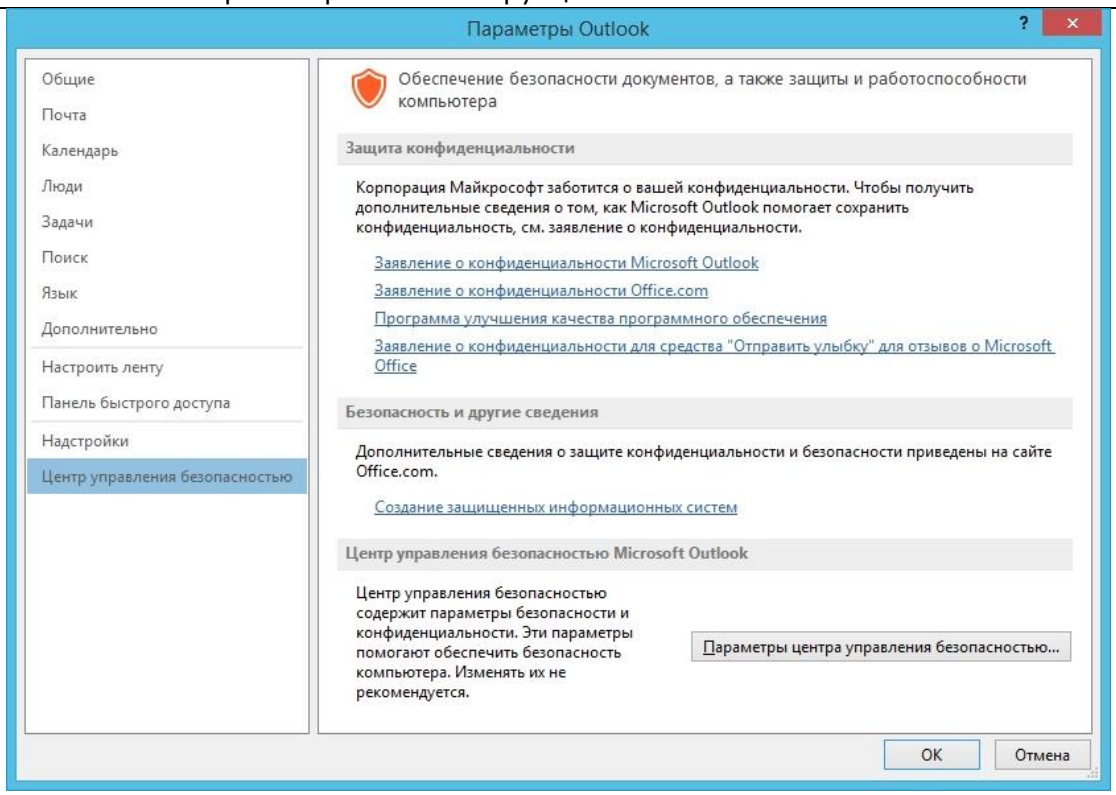


Рисунок 168. Центр управления безопасностью Outlook

Выберите закладку **Защита электронной почты** (**E-mail Security**).

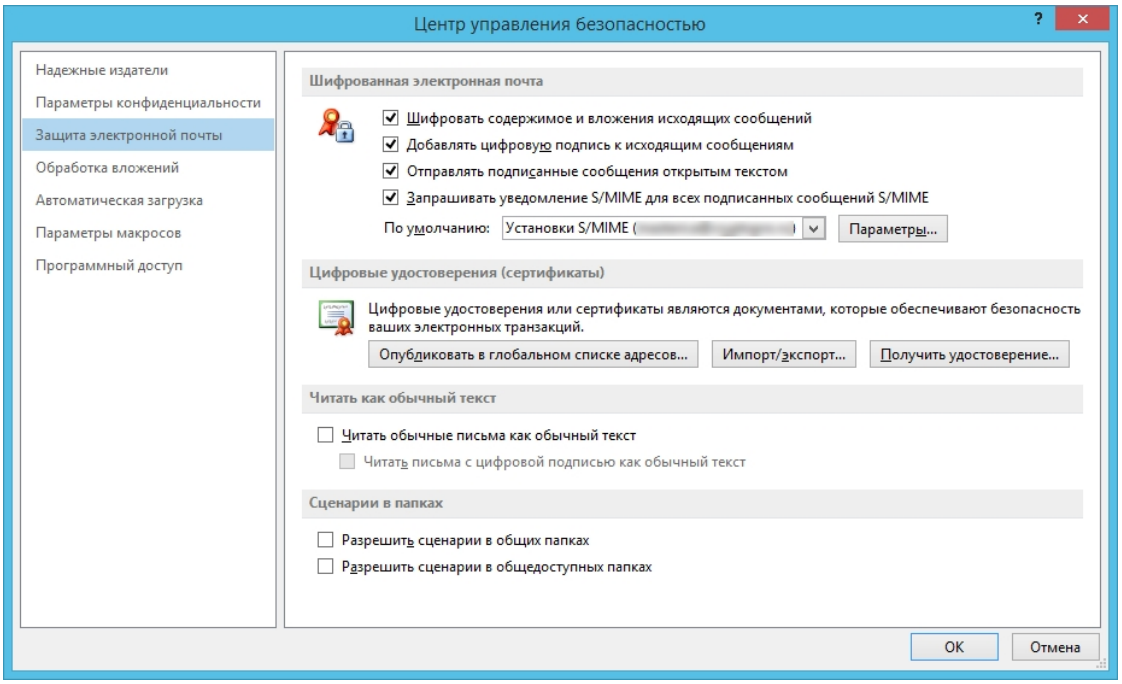


Рисунок 169. Параметры защиты электронной почты

Нажмите **Параметры** (**Settings**).

Выберите личные сертификаты, соответствующие ключам подписи и шифрования, используя кнопку **Выбрать** (**Choose**). Отображаемый диалог позволяет пользователю указать свои личные сертификаты, которые будут использоваться при выборе личных ключей пользователя для формирования электронной цифровой подписи и расшифровки входящих сообщений. Установите флаг **Передавать сертификаты с сообщением** (**Send these certificates with signed messages**).

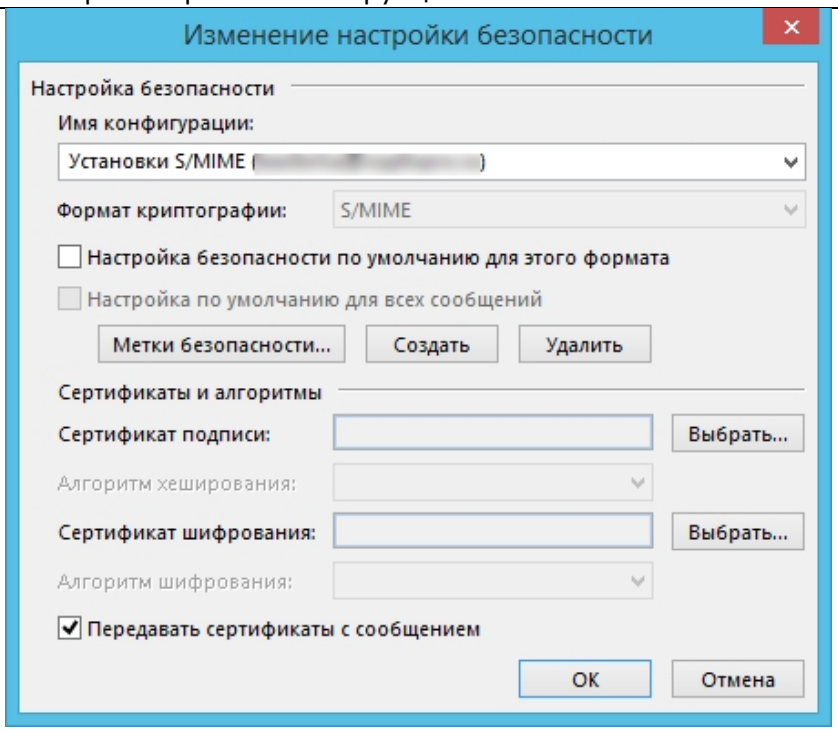


Рисунок 170. Изменение настройки безопасности Outlook

Окно выбора сертификата:

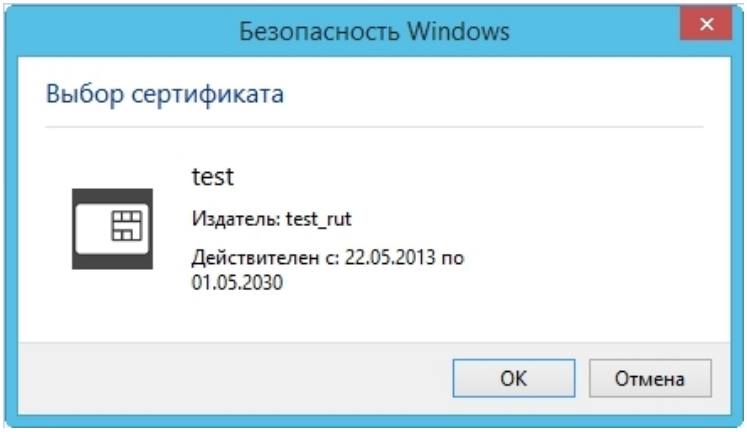


Рисунок 171. Выбор сертификата

После выбора сертификата необходимо указать **Имя конфигурации** (**Security Settings Name**). В противном случае Outlook выдаст ошибку.

В закладке **Защита электронной почты** (**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 электронная цифровая подпись 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.

8.2. 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**).

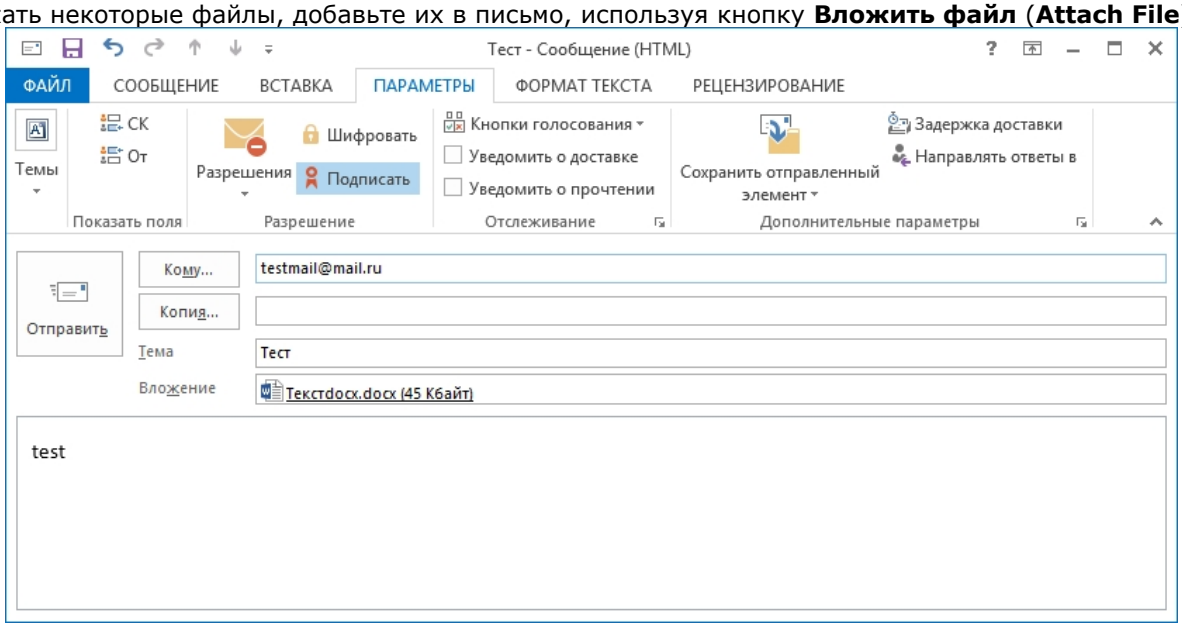


Рисунок 172. Создание подписанного сообщения в Outlook

Для того, чтобы подписать сообщение нажмите на кнопку **Подписать** (**Sign**) в закладке **Параметры** (**Options**).

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 следующее предупреждение, а само сообщение не будет отправлено.

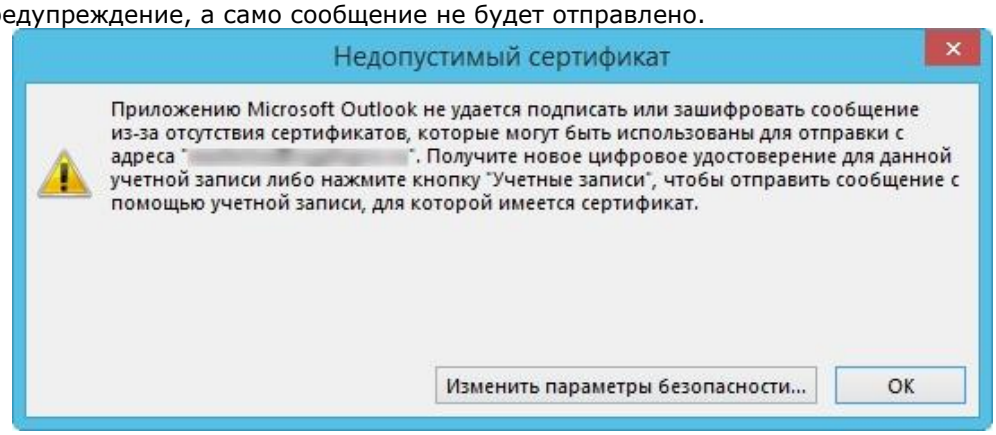


Рисунок 173. Ошибка сертификата отправителя в Outlook

8.3. Получение сертификата открытого ключа абонента для шифрования сообщений

Для шифрования сообщений в адрес других пользователей необходимо предварительно произвести обмен сертификатами. Для этого обычно достаточно переслать подписанное сообщение в адрес требуемого абонента (сообщение посылается вместе с сертификатом отправителя). После получения сообщения и проверки электронной цифровой подписи производится автоматическое добавление адреса отправителя и его сертификата в адресную книгу.

Для контроля добавления выполните следующие действия.

1. Откройте локальную адресную книгу, нажав на значок в нижней части области папок.

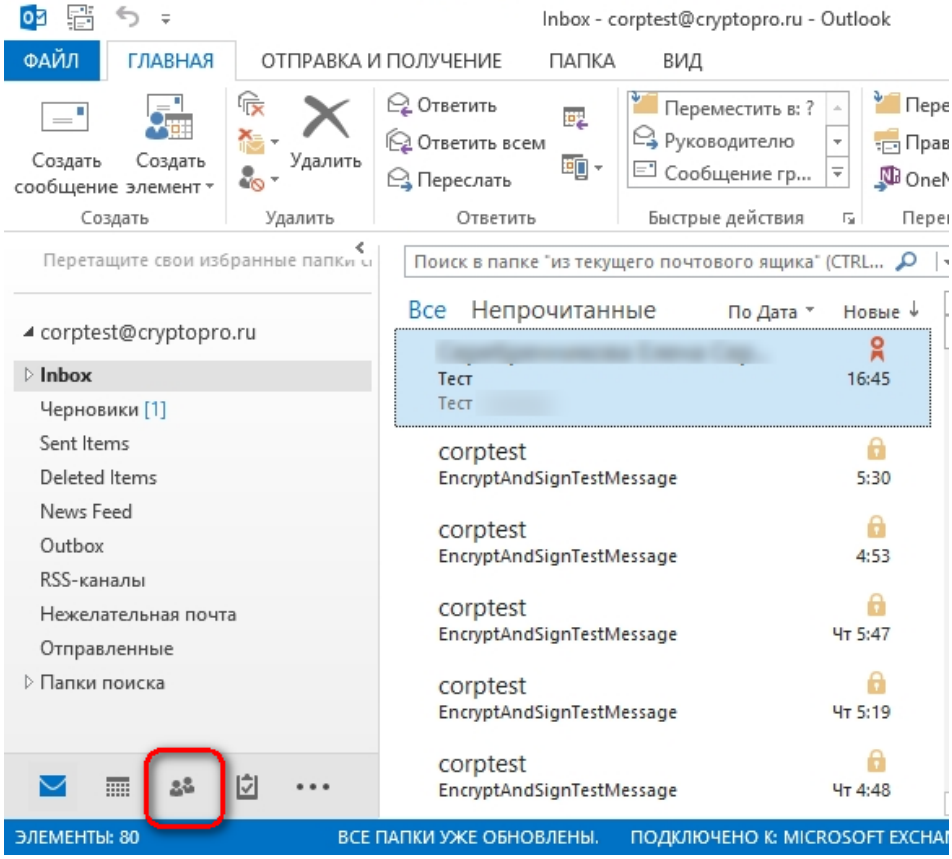
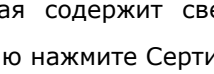


Рисунок 174. Локальная адресная книга Outlook

2. В открывшейся форме выберите нужный контакт и откройте двойным кликом.
3. В форме, которая содержит сведения о контакте, выберите **Показ** (**View**), в открывшемся выпадающем меню нажмите Сертификаты  **(Certificates).**

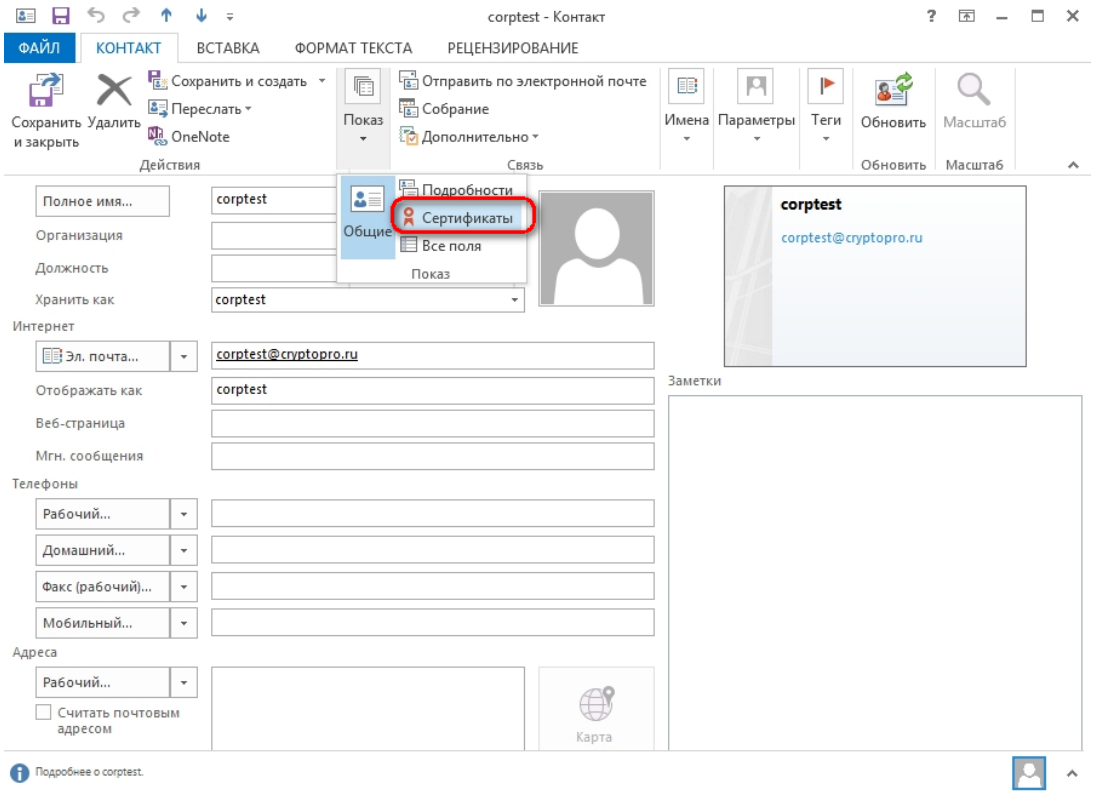


Рисунок 175. Контакт Outlook

В результате откроется список сертификатов, в котором можно увидеть сертификат отправителя.

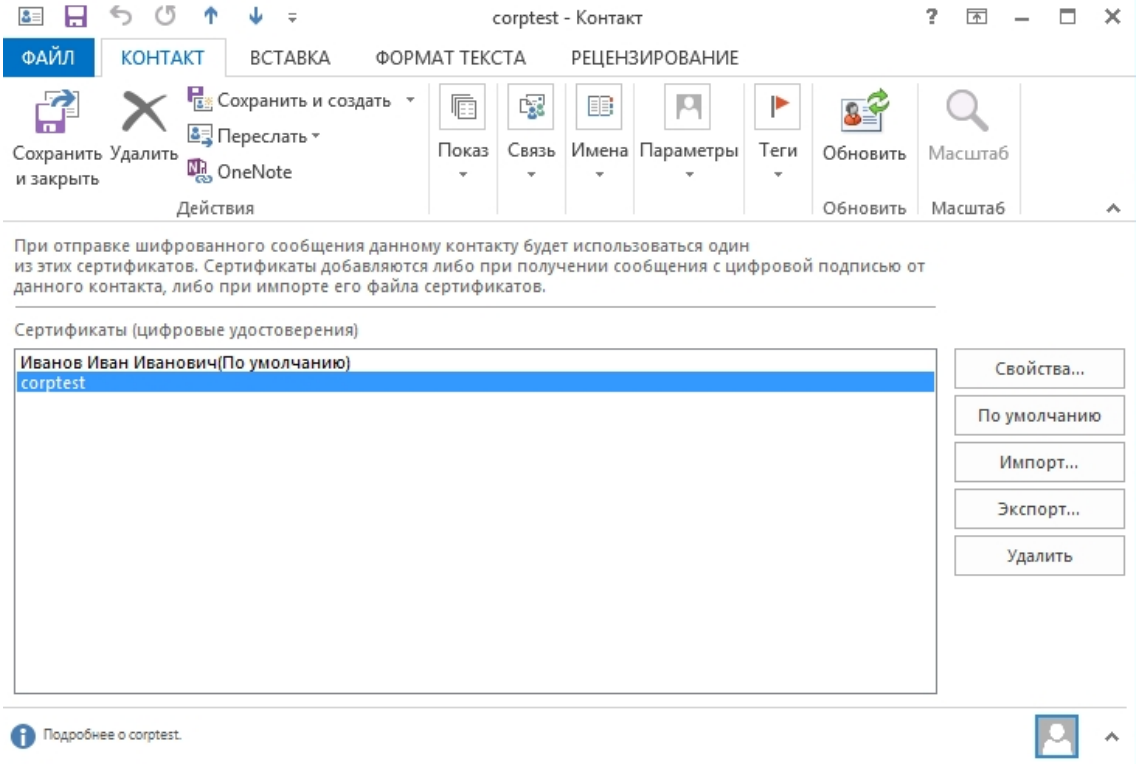


Рисунок 176. Список сертификатов Outlook

После этого нажмите на кнопку **Сохранить и Закрыть** 

(**Save & Close**). Если абонент с таким адресом уже существует, программа предложит, либо добавить новый контакт (**Add new Contact**), либо обновить сведения о выделенном контакте (**Update information of selected Contact**). Выберите второй пункт. При этом в существующий контакт будет добавлен полученный сертификат, а резервная копия будет сохранена в **Deleted Items Folder** (**Удаленные**).

8.4. Отправка шифрованных сообщений

Для создания и отправки шифрованного сообщения нажмите кнопку **Создать** 

(**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**) в закладке **Вставка** (**Insert**). Для отправки сообщения в зашифрованном виде нажмите кнопку **Шифровать** (**Encrypt**).

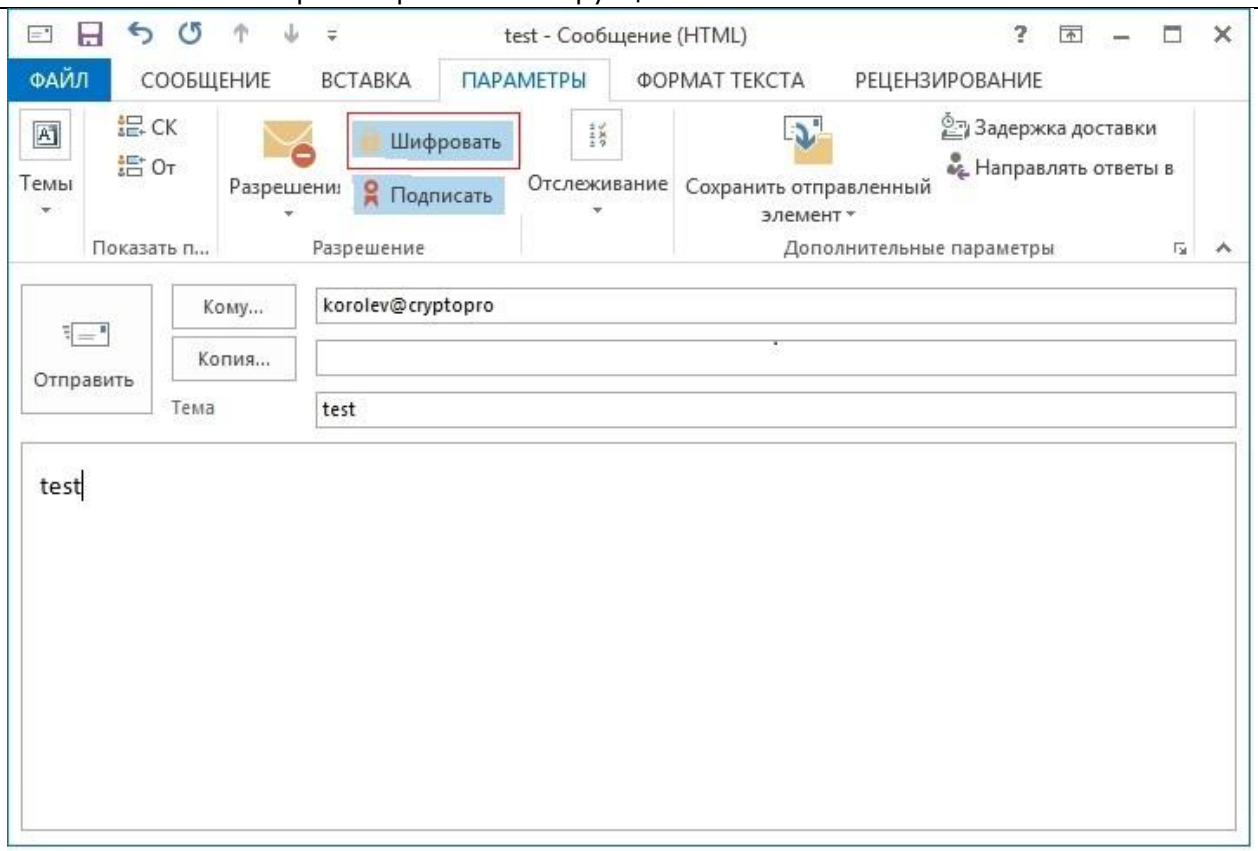


Рисунок 177. Создание зашифрованного сообщения Outlook

После того, как сообщение подготовлено к отправке, нажмите кнопку **Отправить** (**Send**).

При попытке зашифровать письмо на открытом ключе владельца отозванного сертификата, появится следующее предупреждение.

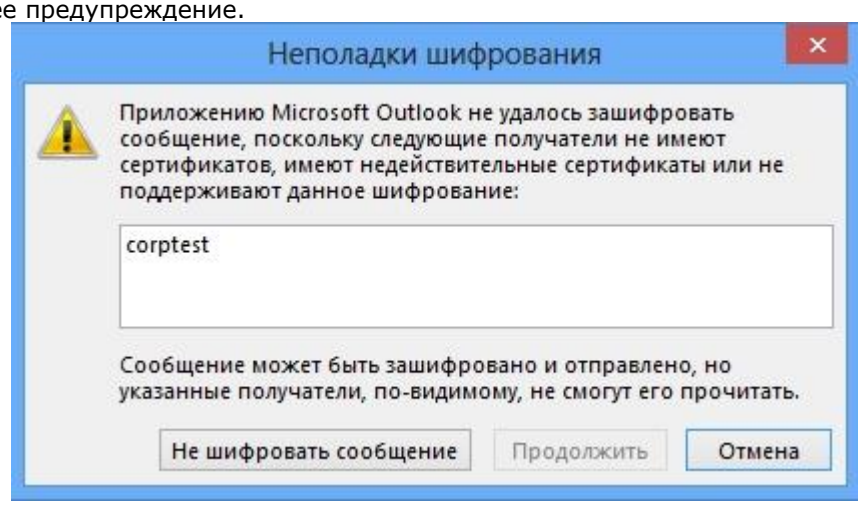


Рисунок 178. Ошибка при шифровании отозванным сертификатом

8.5. Проверка сертификата на отзыв

Для контроля проверки сертификатов на отзыв выполните следующие действия. Откройте полученное подписанное письмо. Нажмите кнопку  – признак подписанного сообщения.

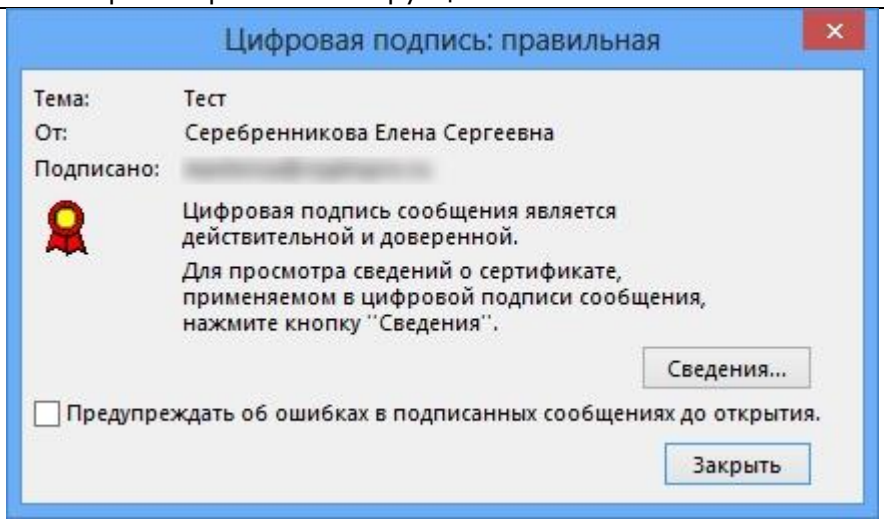


Рисунок 179. Проверка цифровой подписи

Нажмите кнопку **Сведения** (**Details**).
А если открывшееся окно подобно следующему, то СОС не установлен либо срок его действия истек. Обновите СОС, хранящийся в локальном справочнике сертификатов, с использованием доступных средств. Если окно осталось прежним, то сертификат не был отозван.

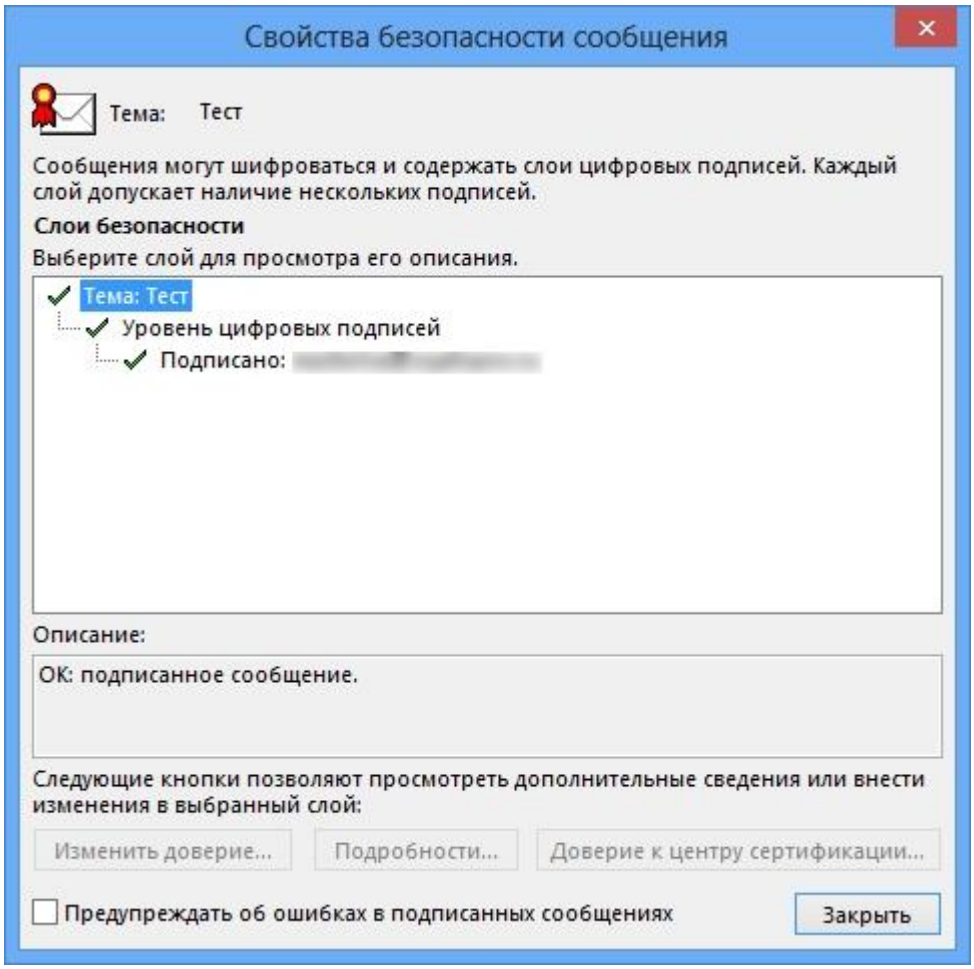


Рисунок 180. Сведения о цифровой подписи в Outlook

Если же СОС обновлен, а письмо подписано отозванным сертификатом, то при нажатии кнопки появится следующее предупреждение:

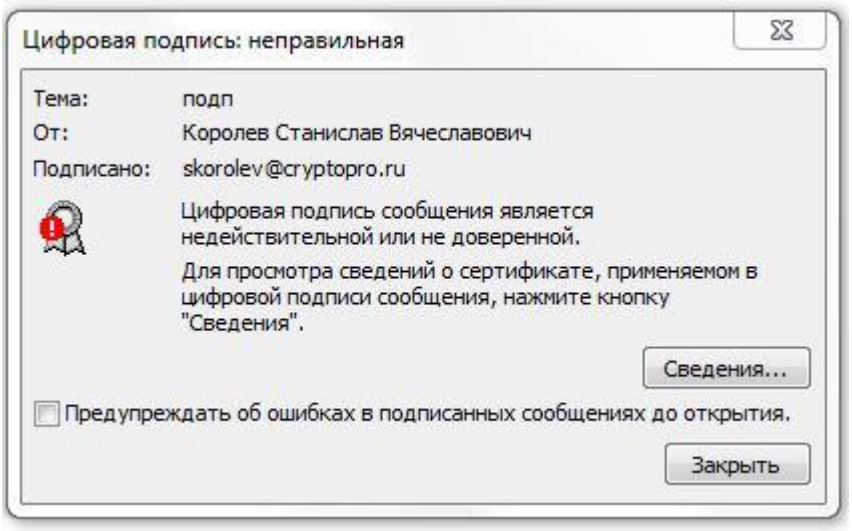


Рисунок 181. Сообщение о недействительной цифровой подписи

Нажмите кнопку **Сведения** (**Details**) для просмотра сведений о сертификате.

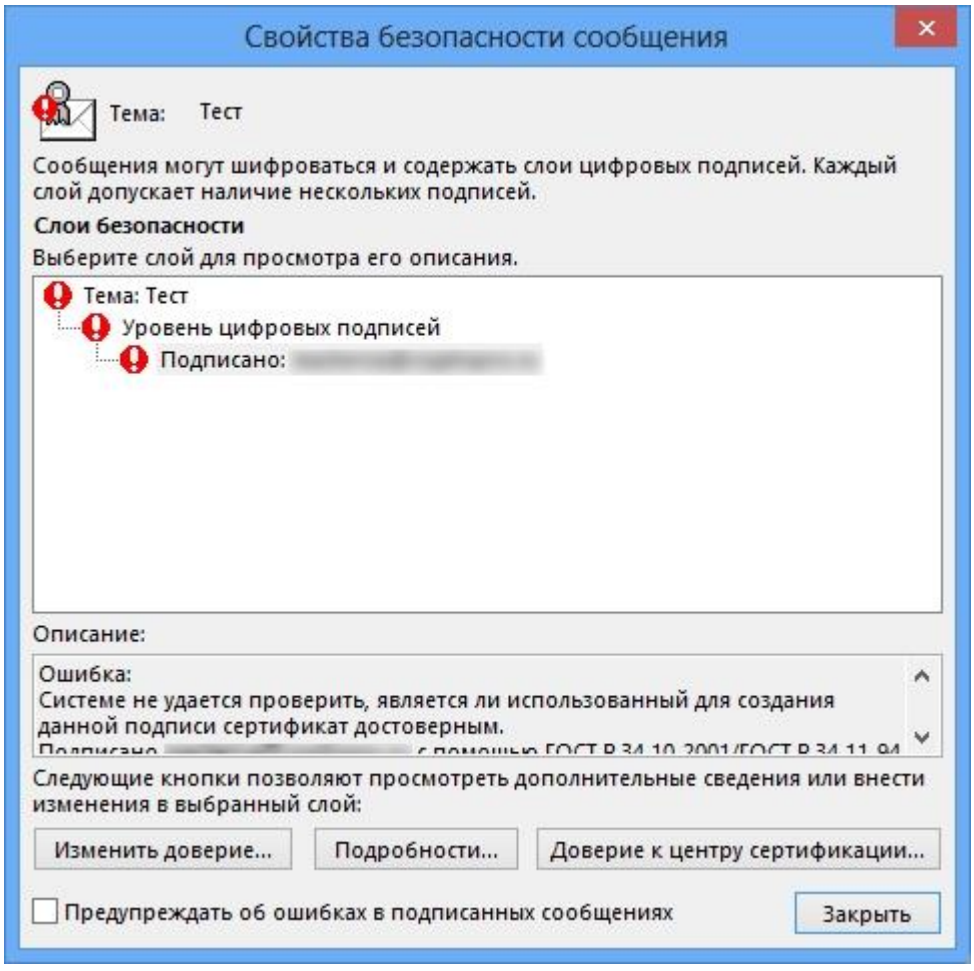


Рисунок 182. Сведения о недействительной цифровой подписи