Технический аспект подключения к компонентам государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет»

Гаврик Константин Юрьевич
Отдел режима секретности
и безопасности информации

ДОКУМЕНТЫ

1. **Руководство по установке и настройке программного обеспечения автоматизированного рабочего места пользователя системы «Электронный бюджет».**

Руководство по установке доступно по адресу в Интернет: http://www.roskazna.ru, раздел «Электронный бюджет» - «Подключение к системе».

Для обеспечения работы в ГИИС «Электронный бюджет» нужно выполнить следующие шаги:

1. Скачать и установить корневой сертификат УЦ Федерального казначейства.
2. Скачать сертификат сервера TLS. Этот сертификат устанавливается на шаге 3.
3. Установить Средство создания защищенного TLS-соединения «КонтинентTLS Клиент».
4. Установить Средство электронной подписи «Jinn-Client».
5. Установить Модуль для работы с электронной подписью «Cubesign».
6. Установить личный сертификат пользователя в хранилище «Личное» (при необходимости).
7. Произвести вход в личный кабинет системы «Электронный бюджет».

Шаг 1.1. Установка корневого сертификата УЦ Федерального казначейства.

1. В веб-обозревателе перейти по адресу в сети Интернет*.
2. На предложение сохранить файл сертификата «Корневой сертификат (квалифицированный).cer» выбрать локальную директорию на АРМ пользователя, в которую будет сохранен файл. Сохранить файл сертификата.
3. Через контекстное меню файла (нажать правой кнопкой мыши по файлу) корневого сертификата УЦ Федерального казначейства выбрать пункт меню «Установить».
4. На экране отобразится мастер импорта сертификатов: Нажать кнопку «Далее>».

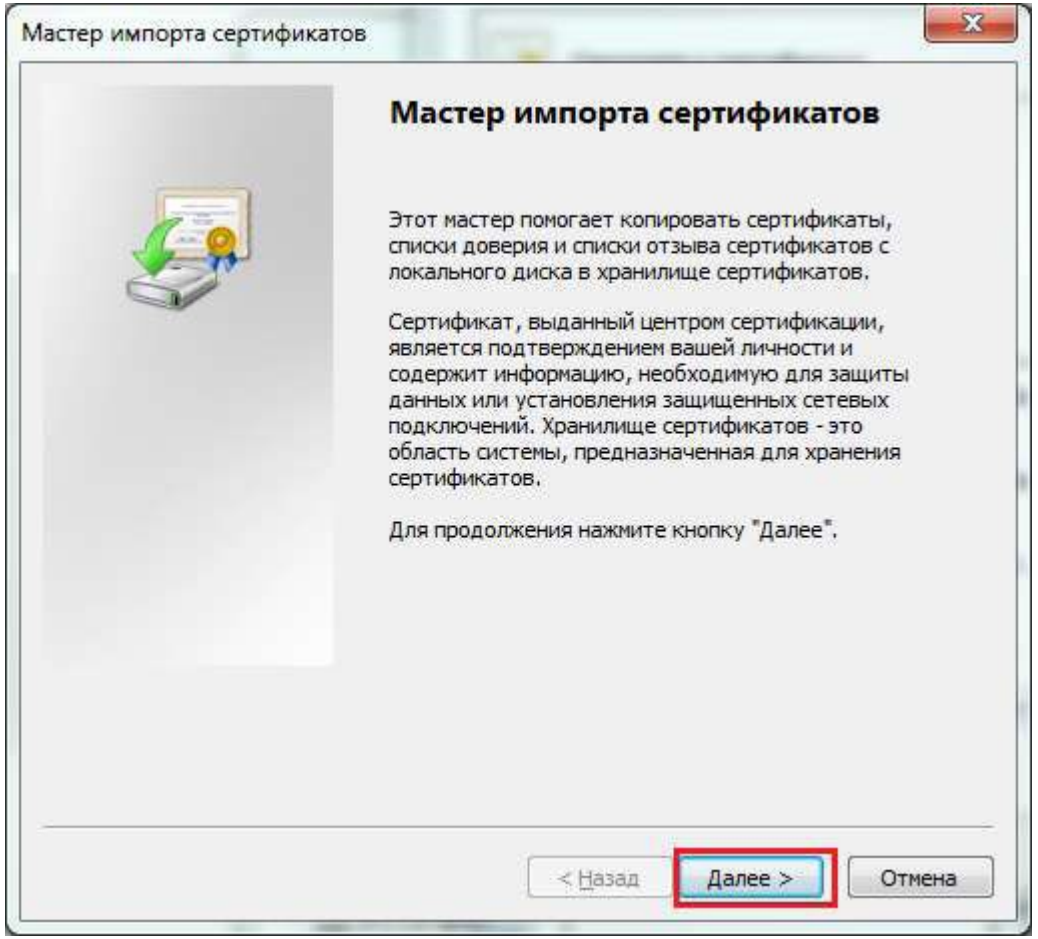

Рисунок . Мастер импорта сертификатов.

* www.roskazna.ru Войти в раздел «Удостоверяющий центр > Корневые сертификаты». Активировать ссылку «Корневой сертификат (квалифицированный)».

Шаг 1.2. Установка корневого сертификата УЦ Федерального казначейства.

4. В окне «Хранилище сертификата» выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».

5. Нажать кнопку «Обзор…».

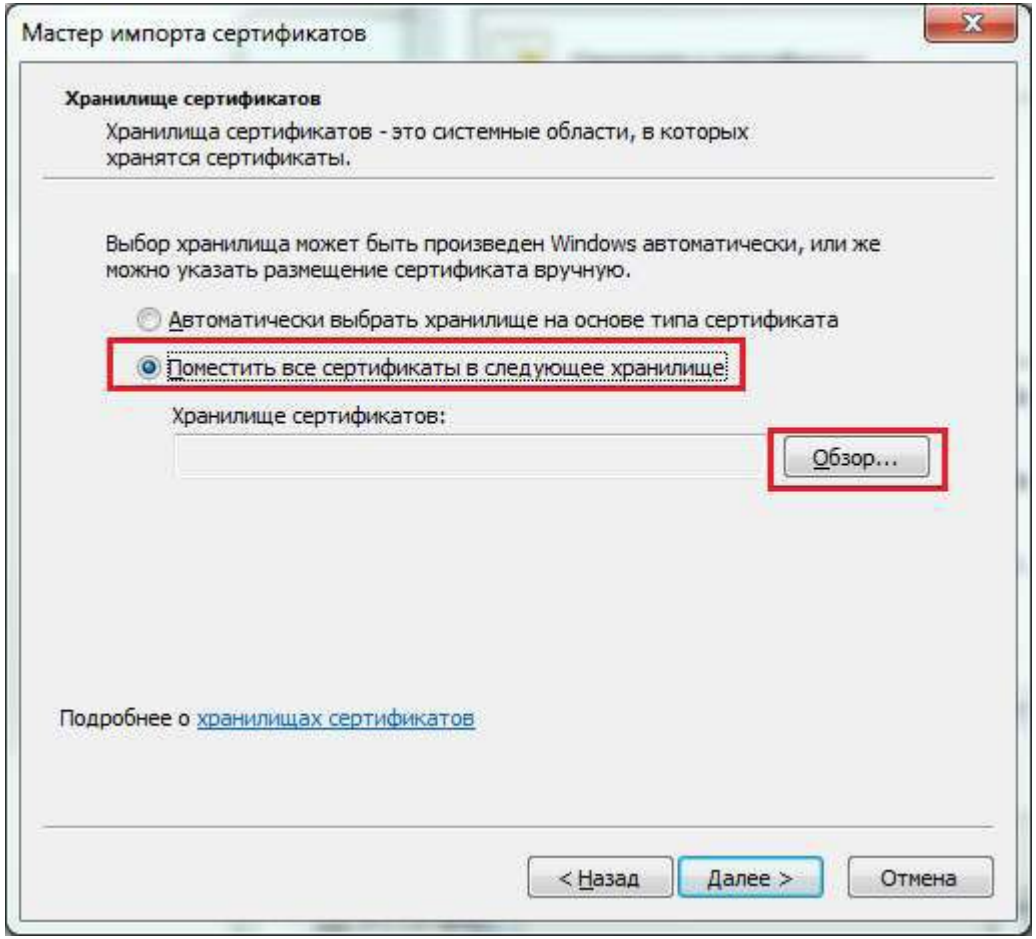

Рисунок. Выбор хранилища сертификата.

Шаг 1.3. Установка корневого сертификата УЦ Федерального казначейства.

6. Отметить поле «Показывать физические хранилища».

7. В окне выбора хранилища сертификатов раскрыть контейнер «Доверенные корневые центры сертификации».

8. В контейнере «Доверенные корневые центры сертификации» выбрать вложенный контейнер «Локальный компьютер».

9. Нажать кнопку «Ок».

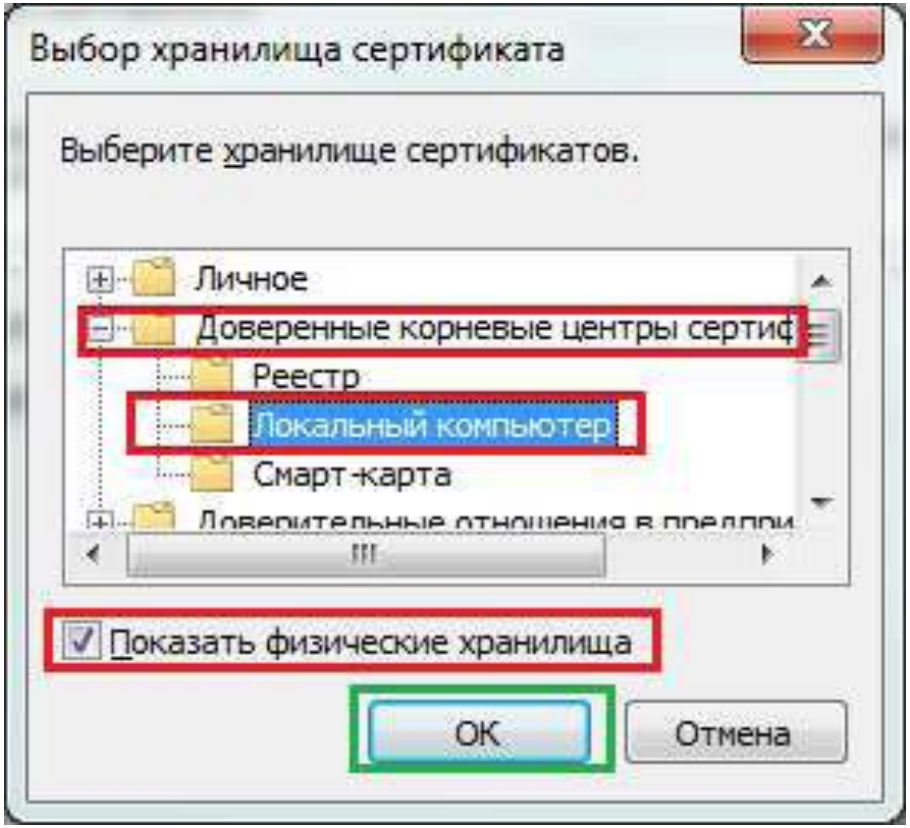

Рисунок. Выбор хранилища сертификата. Локальный компьютер.

Шаг 1.4. Установка корневого сертификата УЦ Федерального казначейства.

10. Нажать кнопку «Далее>».

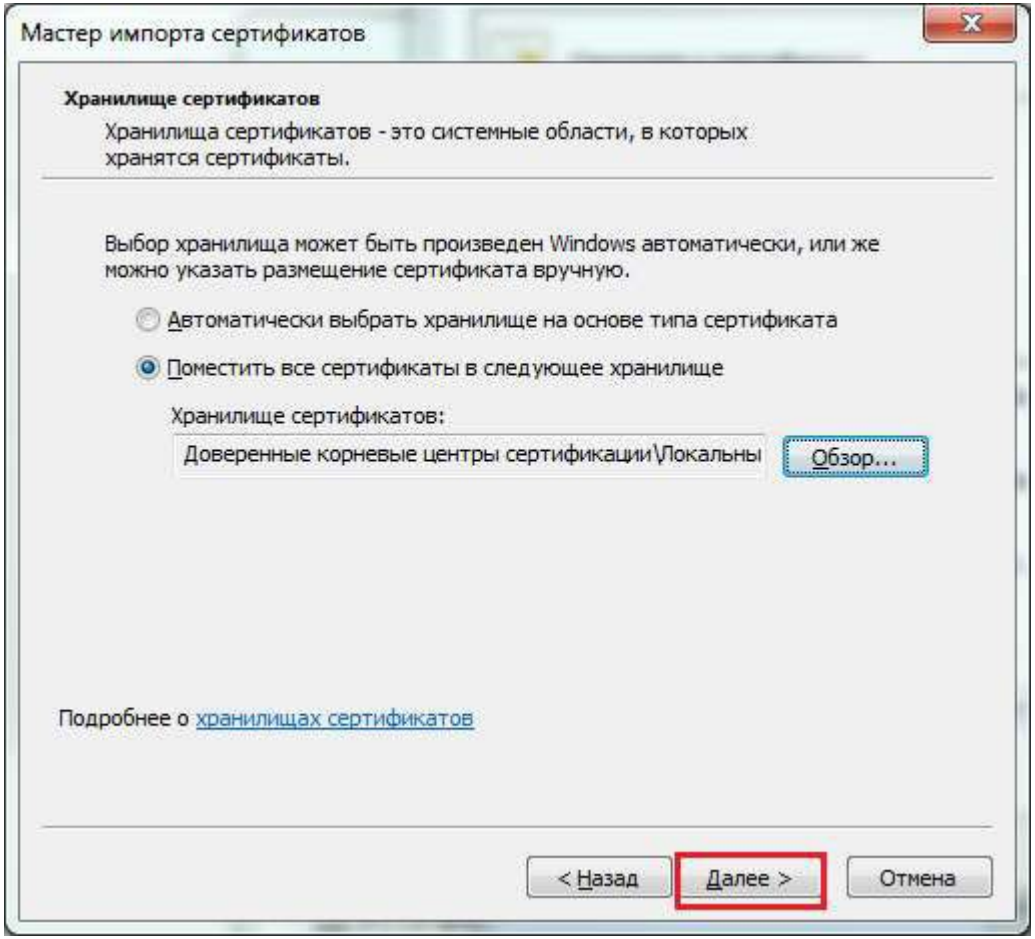

Рисунок. Выбор хранилища сертификата. Установка.

Шаг 1.5. Установка корневого сертификата УЦ Федерального казначейства.

11. Нажать кнопку «Готово».

12. В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен».

13. Нажать кнопку «ОК».

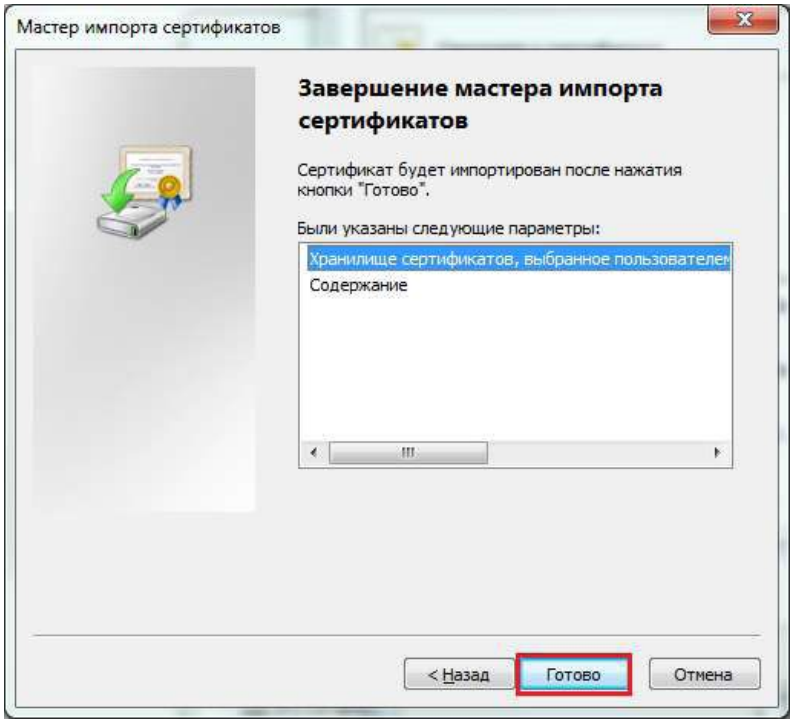

Рисунок . Завершение установки.

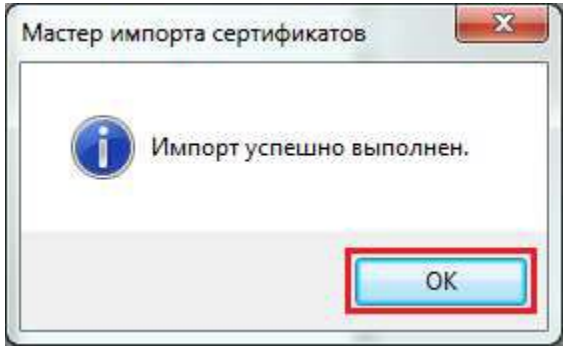

Рисунок . Успешный импорт сертификата.

Шаг 2. Загрузка сертификата сервера TLS.

1. Открыть в веб-обозревателе официальный сайт Федерального казначейства, перейдя по адресу в сети Интернет: www.roskazna.ru

2. Перейти в раздел «Электронный бюджет > Подключение к системе».

3. Активировать ссылку «Ссылка для скачивания сертификата сервера

“Континент TLS VPN”».

4. На предложение сохранить файл сертификата «Федеральное казначейство__.cer» выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.

5. Сохранить файл сертификата сервера TLS.

Шаг 3.1. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

1. Активируйте ссылку «Континент TLS Клиент» в едином меню установщика ПО «Континент TLS Клиент» На экране отобразится стартовое окно мастера установки компонента.
2. Нажать кнопку «Далее». На экране появится окно лицензионного соглашения.

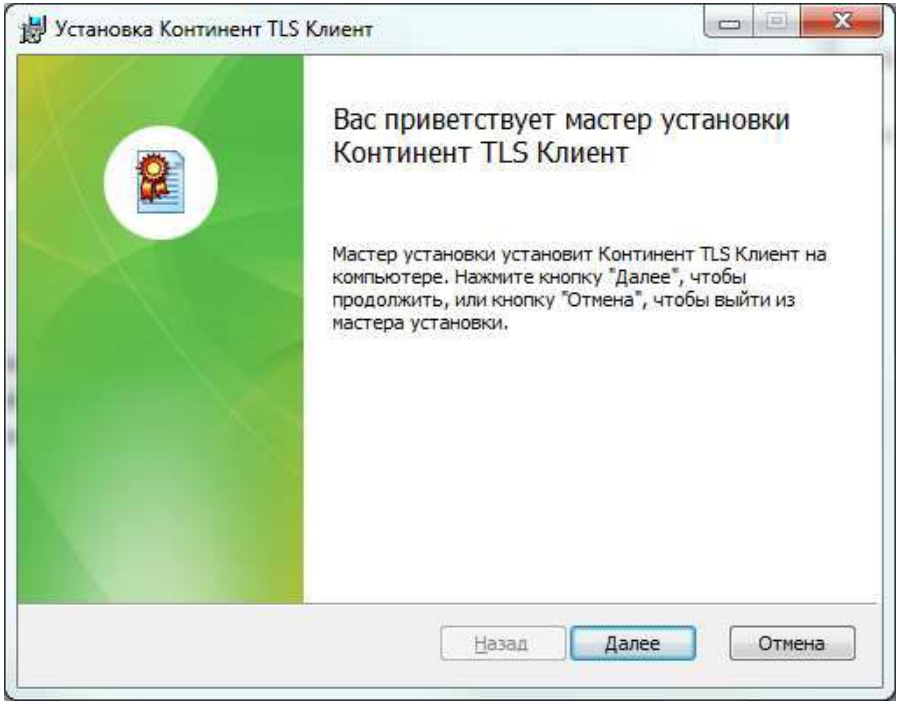

Рисунок . Стартовое окно мастера установки ПО «Континент TLS Клиент».

Шаг 3.2. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

3. Поставьте отметку в поле «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее». На экране появится окно ввода лицензионного ключа.

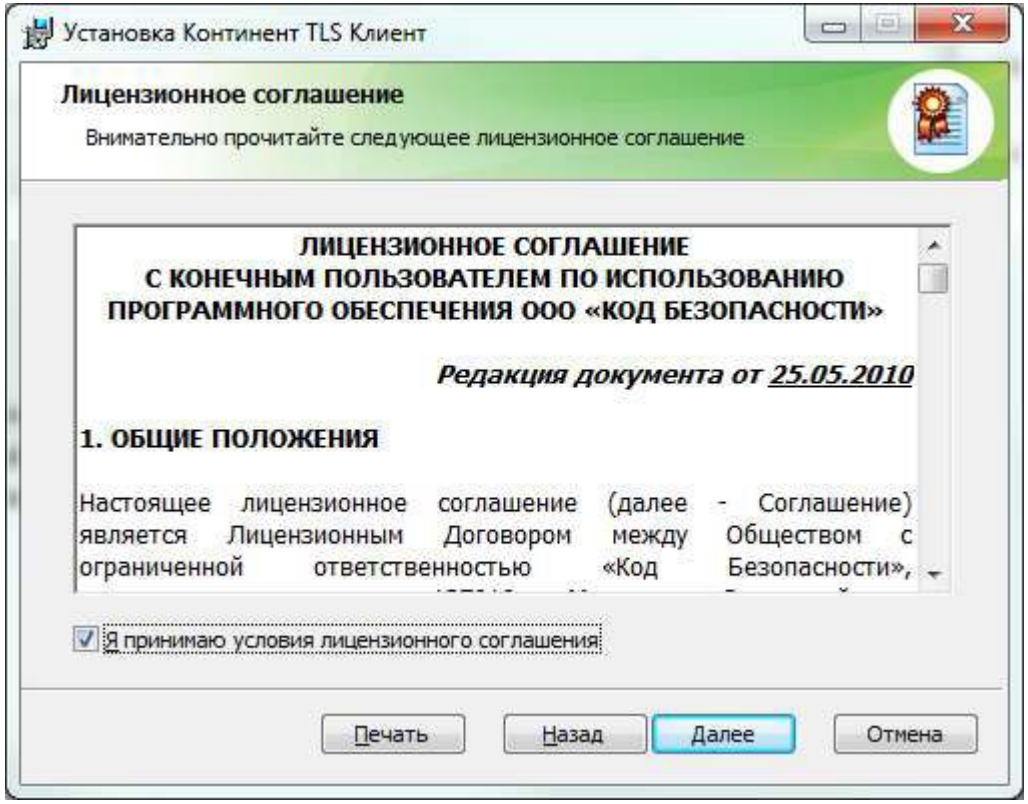

Рисунок . Окно лицензионного соглашения ПО «Континент TLS Клиент».

Шаг 3.3. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

4. Введите лицензионный ключ и нажмите кнопку «Далее». На экране появится диалог выбора пути установки ПО «Континент TLS Клиент».

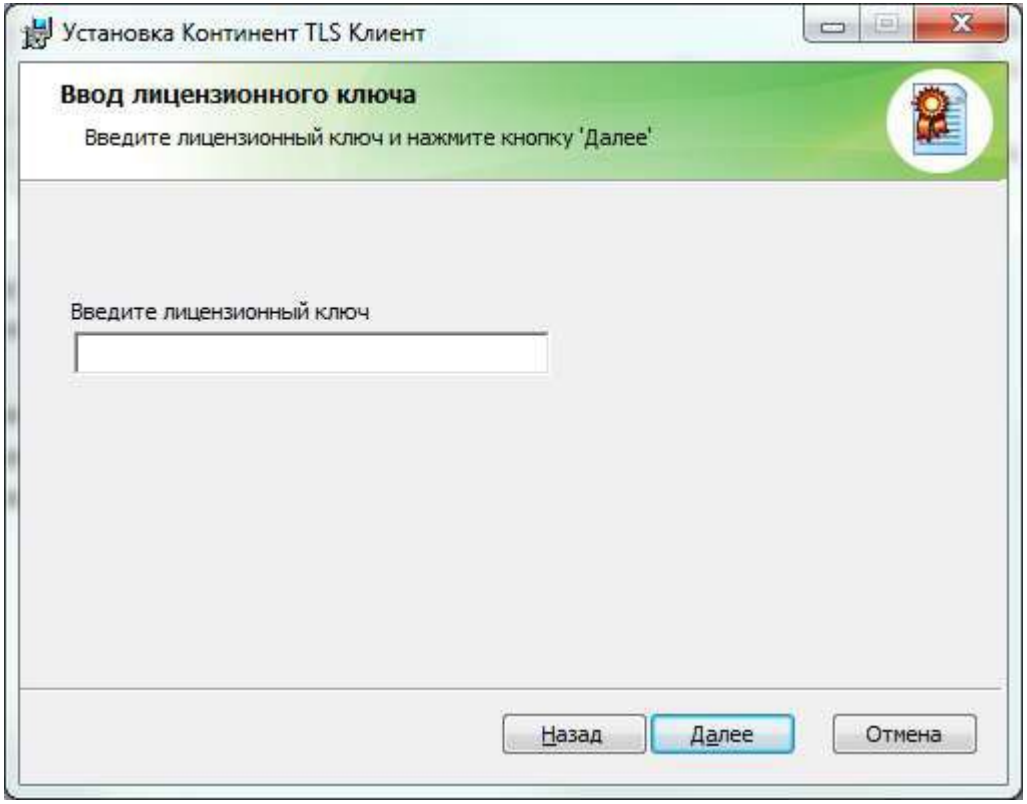

Рисунок . Окно ввода лицензионного ключа ПО «Континент TLS Клиент».

Шаг 3.4. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

5. Оставьте путь установки по умолчанию. Нажмите кнопку «Далее». На экране появится диалог «Запуск конфигуратора».

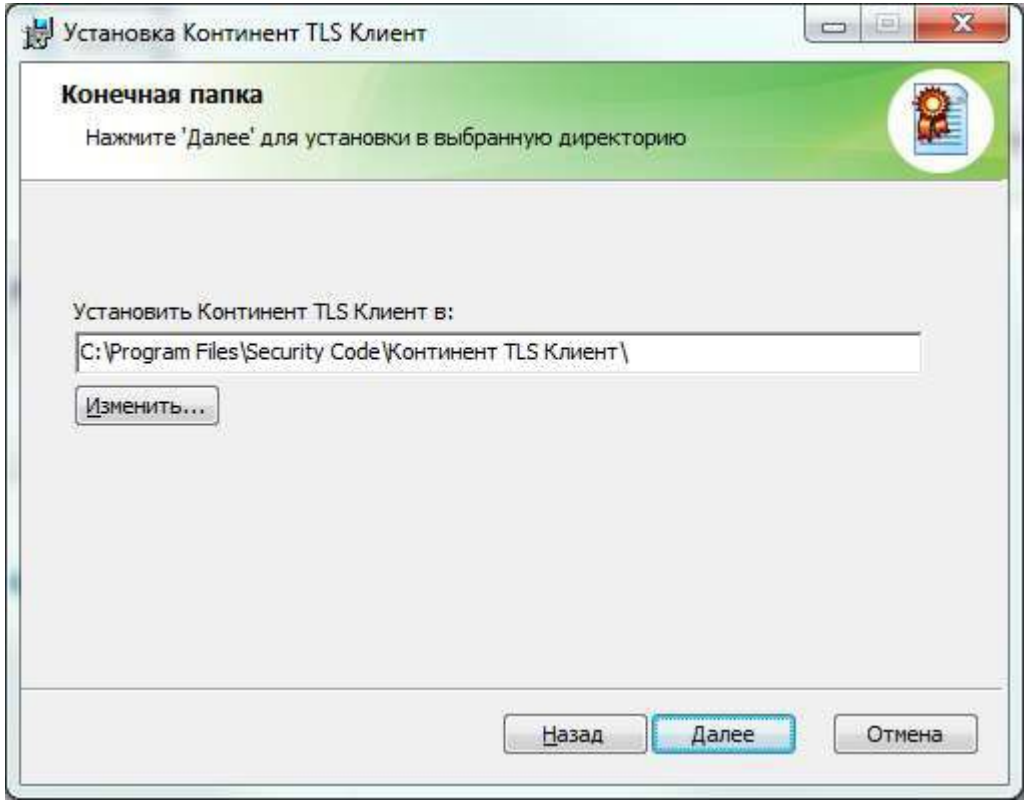

Рисунок . Окно выбора пути установки ПО «Континент TLS Клиент».

Шаг 3.5. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

6. Установите отметку в поле «Запустить конфигуратор после завершения установки».

7. Нажмите кнопку «Далее». На экране появится окно с сообщением о готовности к установке.

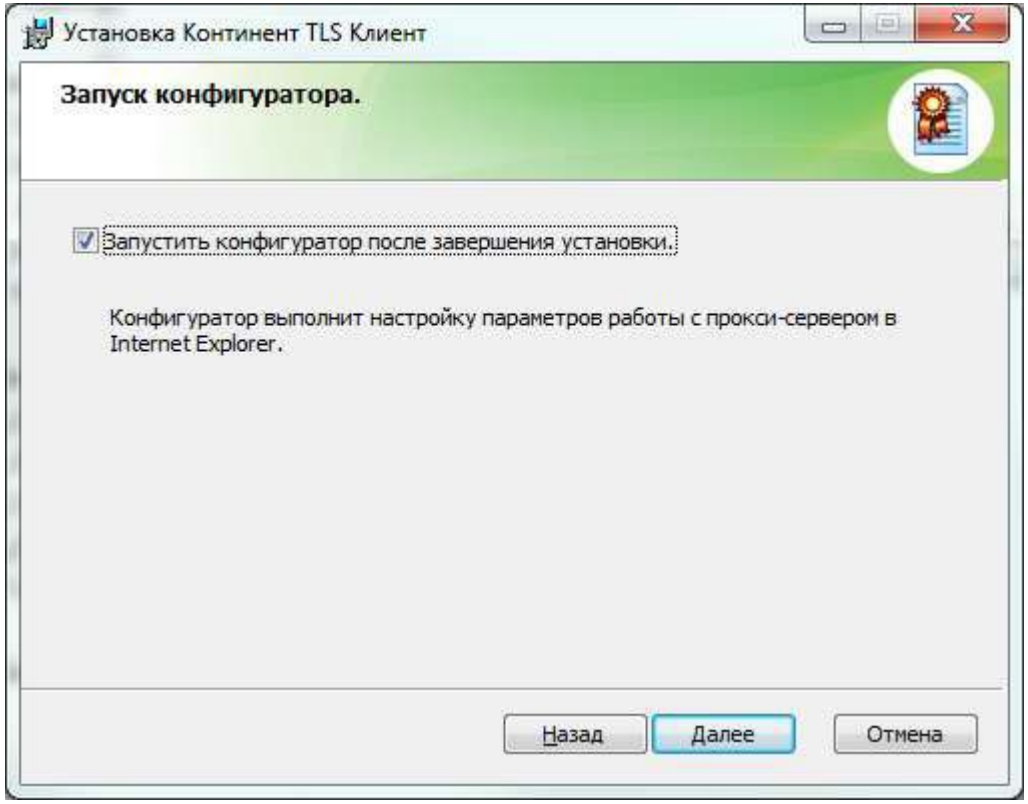

Рисунок . Окно запуска конфигуратора ПО «Континент TLS Клиент».

Шаг 3.6. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

8. Нажмите кнопку «Установить». Начнется установка компонента.

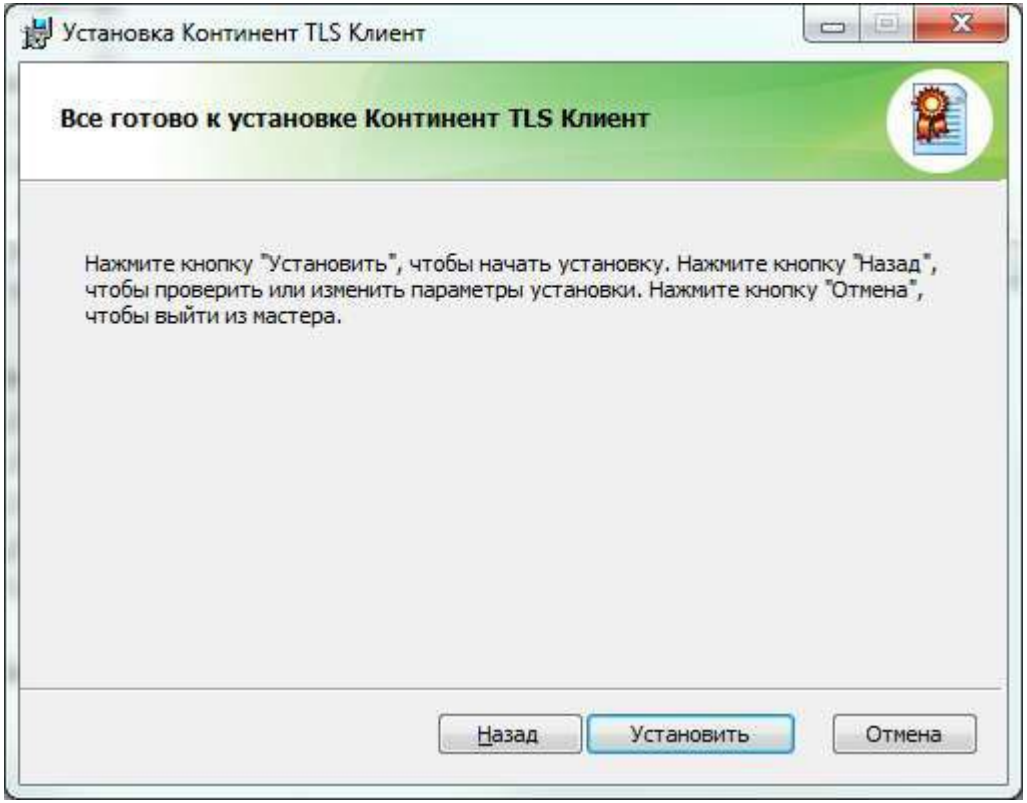

Рисунок . Окно готовности к установке ПО «Континент TLS Клиент».

Шаг 3.7. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

9. На экране отобразится диалог настройки ПО «Континент TLS Клиент».

10. В разделе «Настройки Континент TLS Клиента» значение «Порт» оставить по умолчанию, равное 8080.

11. В разделе «Настройки защищаемого сервера» в поле «Адрес» задать имя сервера TLS: lk.budget.gov.ru.

12. В разделе «Настройки защищаемого сервера» в поле «Сертификат» указать файл сертификата сервера TLS, скопированный в локальную директорию на шаге 2.

13. Если в АРМ пользователя не используется внешний прокси-сервер, нажать кнопку «ОК».

14. В противном случае, указать адрес и порт используемого внешнего прокси-сервера организации.

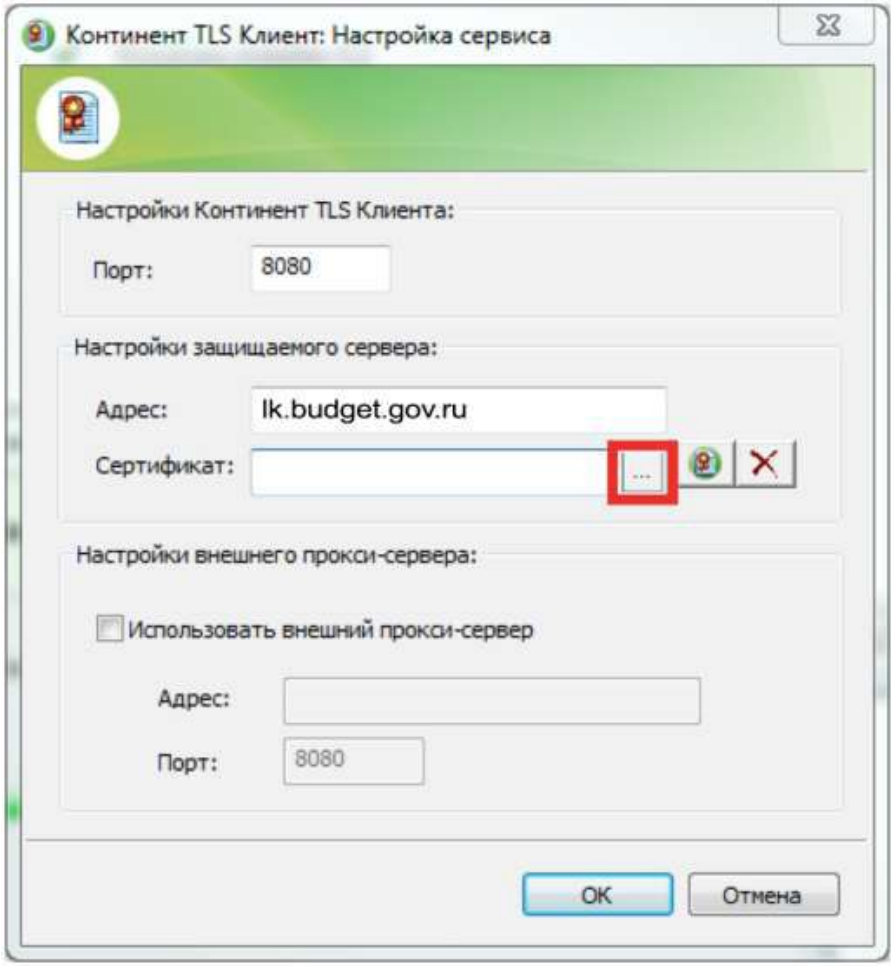

Рисунок . Настройка ПО «Континент TLS Клиент».

Шаг 3.9. Установка средства создания защищенного TLS-соединения «Континент TLS клиент».

11. Нажать кнопку «Готово».

12. На экране отобразится диалог о необходимости перезагрузки АРМ пользователя.

13. Нажать кнопку «Нет».

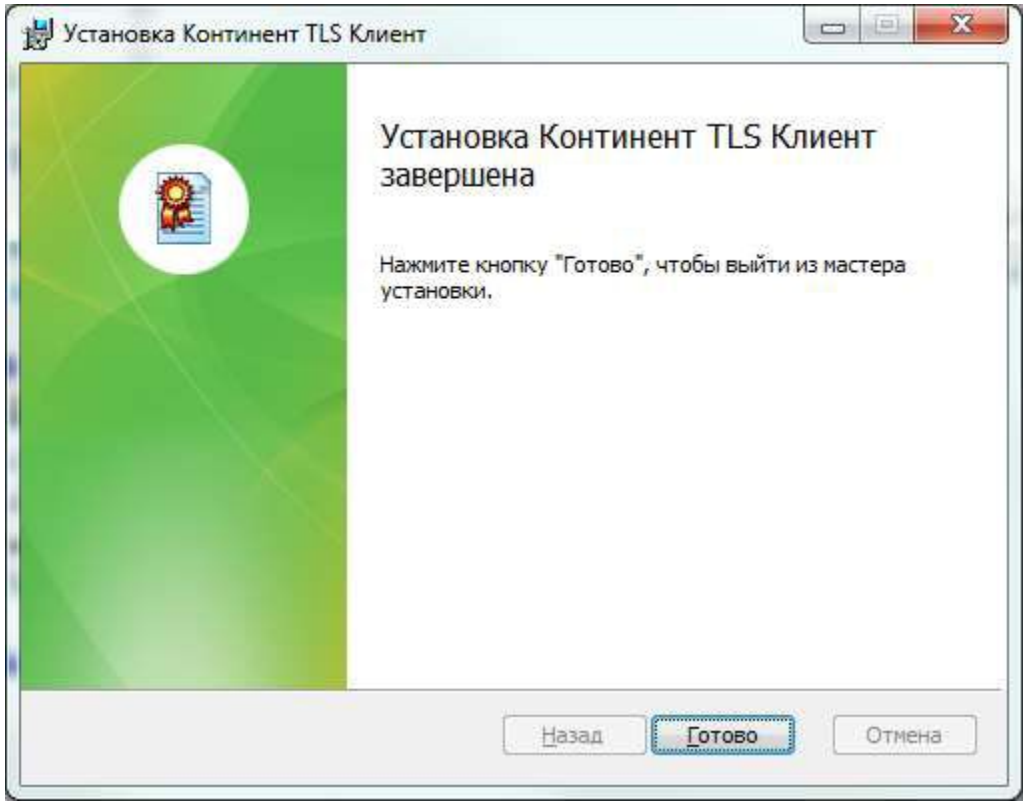

Рисунок . Диалог завершения установки ПО «Континент TLS Клиент».

Шаг 4.1. Установка средства электронной подписи «Jinn-Client».

1. В меню единого установщика ПО «Jinn-Client» активировать ссылку «Jinn-Client». На экране отобразится диалог приветствия установщика ПО «Jinn-Client».

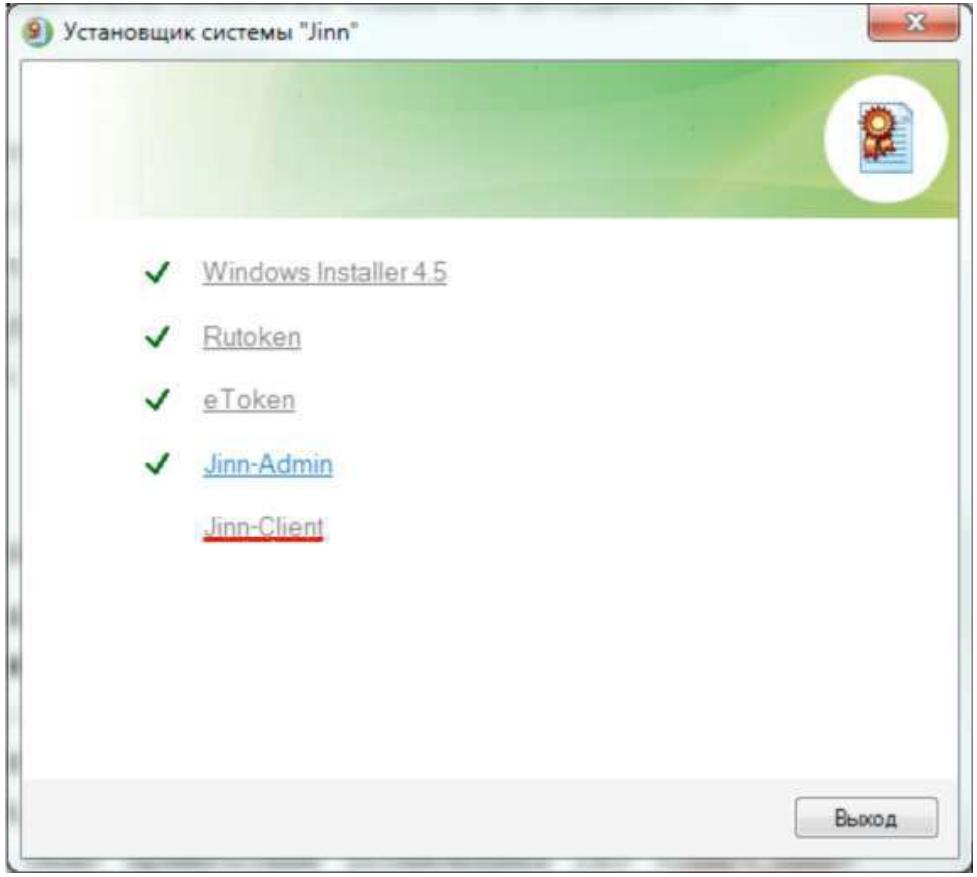

Рисунок . Меню единого установщика ПО «Jinn-Client»

Шаг 4.2. Установка средства электронной подписи «Jinn-Client».

2. Для продолжения установки нажмите кнопку «Далее».

3. В появившемся диалоге лицензионного соглашения отметить пункт «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее».

4. На экране отобразится диалог ввода лицензионного ключа.

5. Введите лицензионный ключ и нажмите кнопку «Далее».

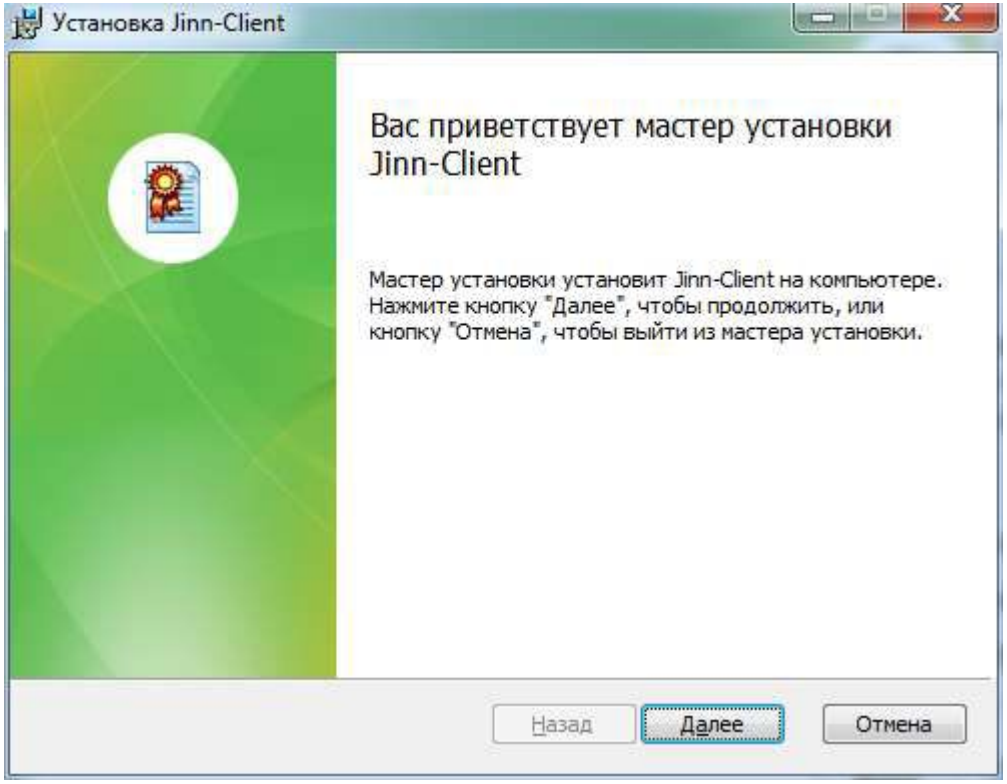

Рисунок . Окно приветствия установщика Jinn-Client

Шаг 4.3. Установка средства электронной подписи «Jinn-Client».

6. Оставьте путь установки по умолчанию либо измените на требуемый. Нажмите кнопку «Далее».

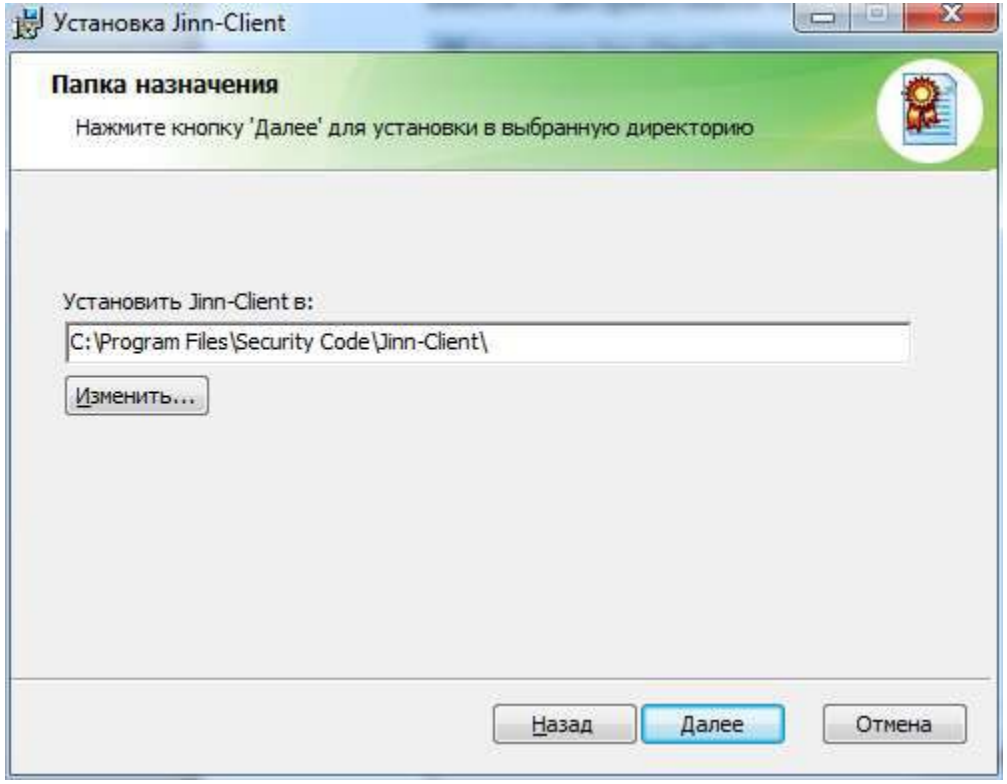

Рисунок . Окно выбора пути установки Jinn-Client

Шаг 4.4. Установка средства электронной подписи «Jinn-Client».

7. В диалоге настройки параметров Jinn-Client ничего не изменяя нажмите кнопку «Далее».

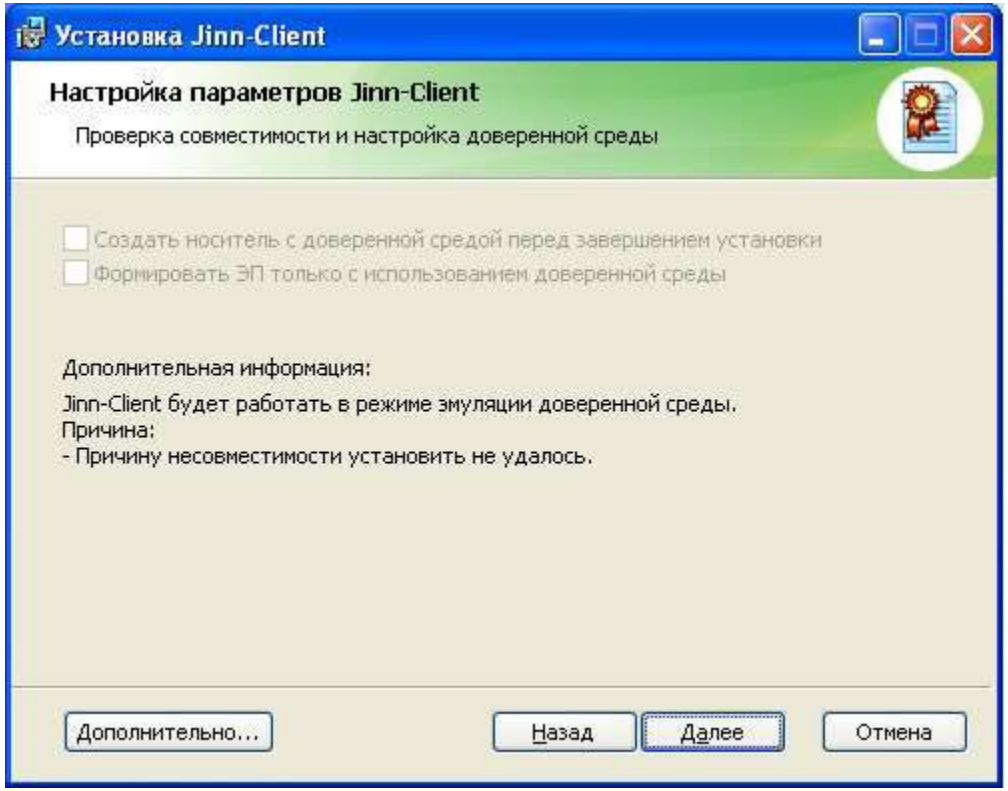

Рисунок . Окно настройки параметров Jinn-Client

Шаг 4.5. Установка средства электронной подписи «Jinn-Client».

8. Нажмите кнопку «Установить». По завершению установки на экран будет выведен диалог об успешном завершении.

9. Нажмите кнопку «Готово».

10. На экране отобразится диалог о необходимости перезагрузки АРМ пользователя. Нажать кнопку «Нет».

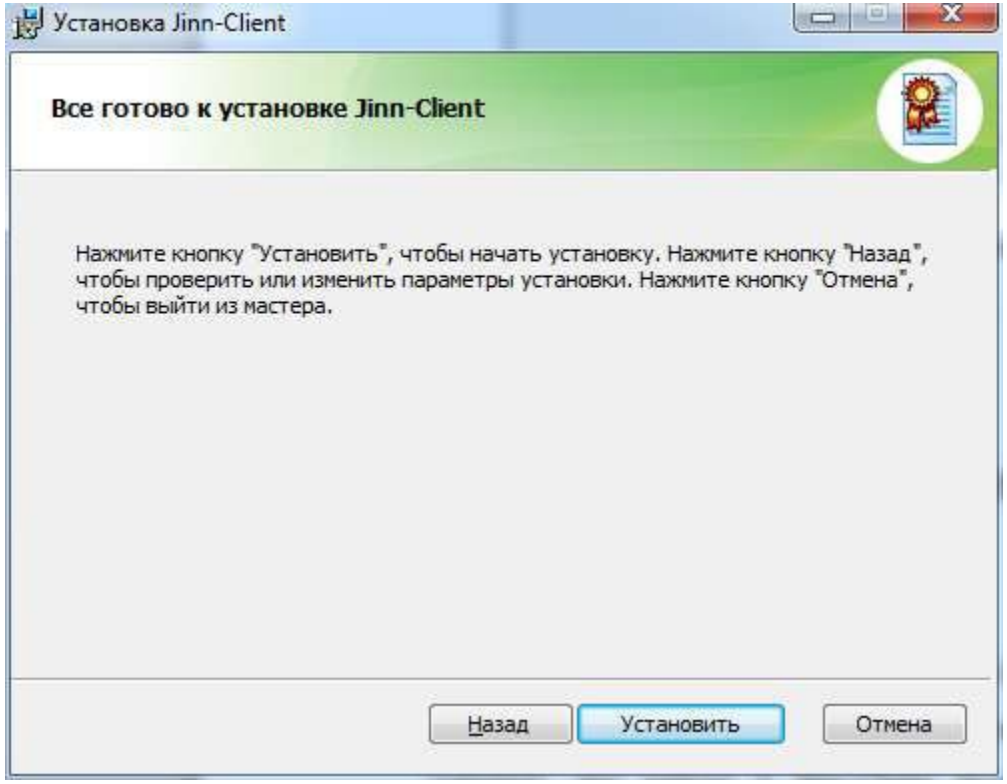

Рисунок . Сообщение о готовности к установке Jinn-Client

Шаг 5.1. Установка модуля для работы с электронной подписью «Cubesign».

1. В составе дистрибутива ПО «Jinn-Client» осуществить запуск исполняемого файла «Cubesign».

2. На экране отобразится диалог приветствия установщика модуля. Нажать кнопку «Далее».

3. На экране отобразится окно лицензионного соглашения.

4. Принять условия лицензионного соглашения поставив галочку в соответствующем поле и нажмите «Далее».

5. На экране отобразится диалог расположения файлов установки модуля. Установить компонент средства подписи в папку предложенную по умолчанию и нажмите «Далее».

7. Подтвердить начало установки, нажав кнопку «Установить».

8. Дождитесь окончания процесса установки, нажмите «Готово». Перезагрузите АРМ.

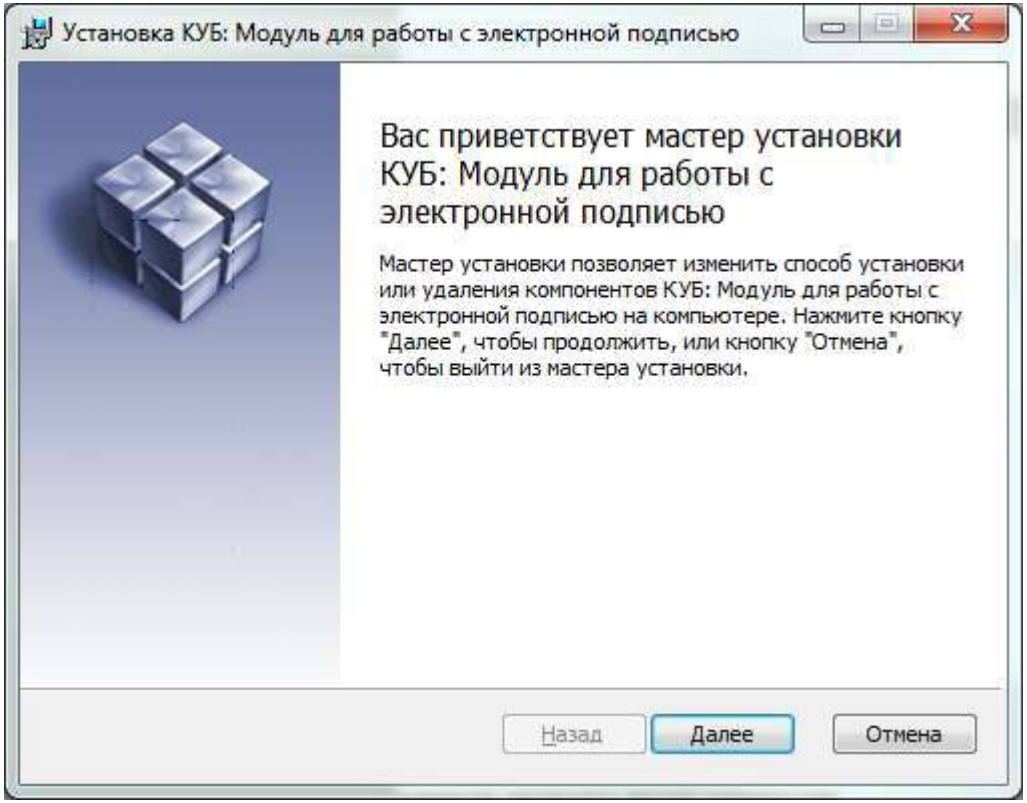

Рисунок . Диалог приветствия установщика модуля

Шаг 5.2. Установка модуля для работы с электронной подписью «Cubesign» (при необходимости).

9. В случае появления диалога о блокировке активного содержимого личного кабинета, в правом верхнем углу нажать кнопку «Разрешить…».

10. Во всплывающем диалоге нажать кнопку «Разрешить и запомнить».

11. В верхней части окна в предупреждающем сообщении о незагруженном элементе управления активировать предлагаемую ссылку.

12. В диалоге сохранения файла нажать кнопку «Сохранить файл».

13. Выполнить запуск сохраненного файла «cubesign.msi».

14. Выполнить перезапуск веб-обозревателя

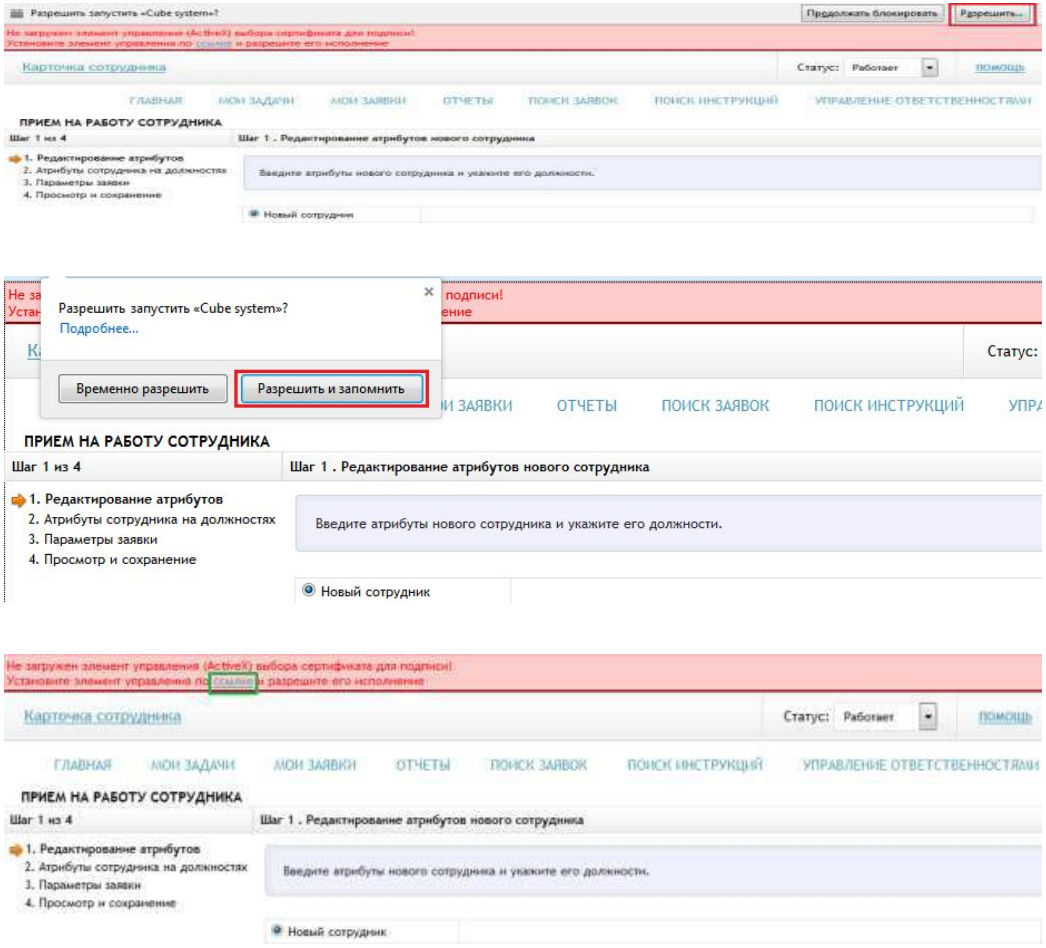

Рисунок . Действия для установки «Cubesign» в web-обозревателях

Шаг 6.1. Установка личного сертификата пользователя в хранилище «Личное» (при необходимости).

1. Через контекстное меню файла сертификата пользователя выбрать пункт меню «Установить сертификат».

2. На экране отобразится мастер импорта сертификатов.

3. Нажать кнопку «Далее>».

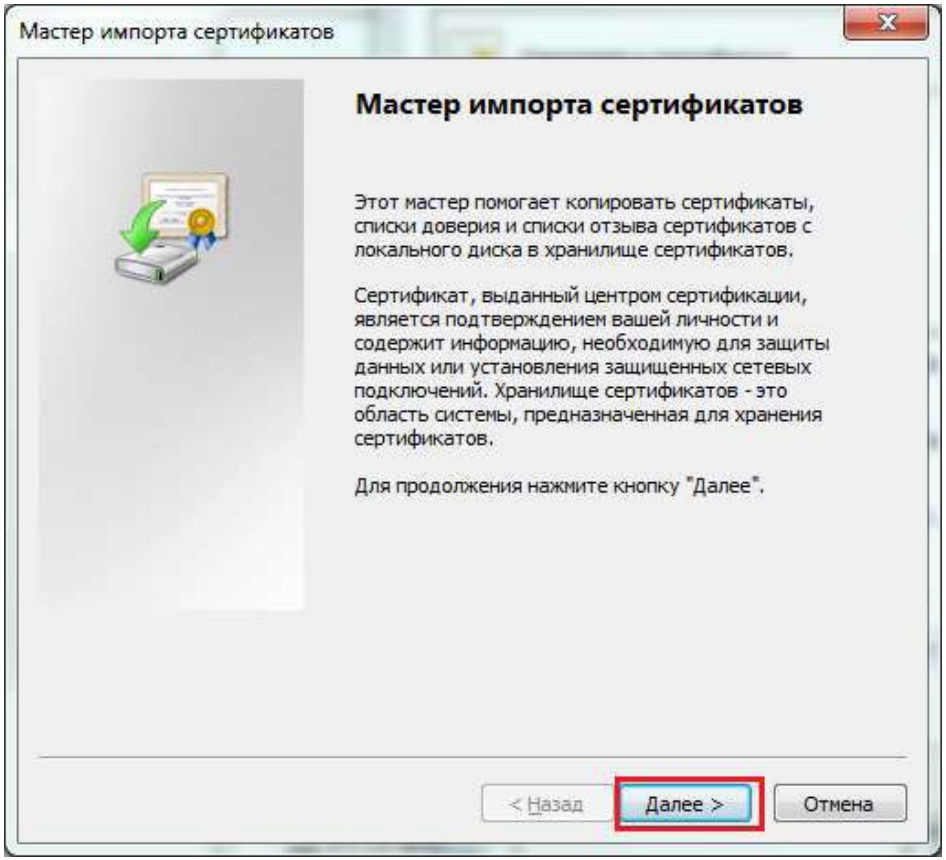

Рисунок . Мастер импорта сертификатов.

Шаг 6.2. Установка личного сертификата пользователя в хранилище «Личное» (при необходимости).

4. В окне «Хранилище сертификата» выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».

5. Нажать кнопку «Обзор…».

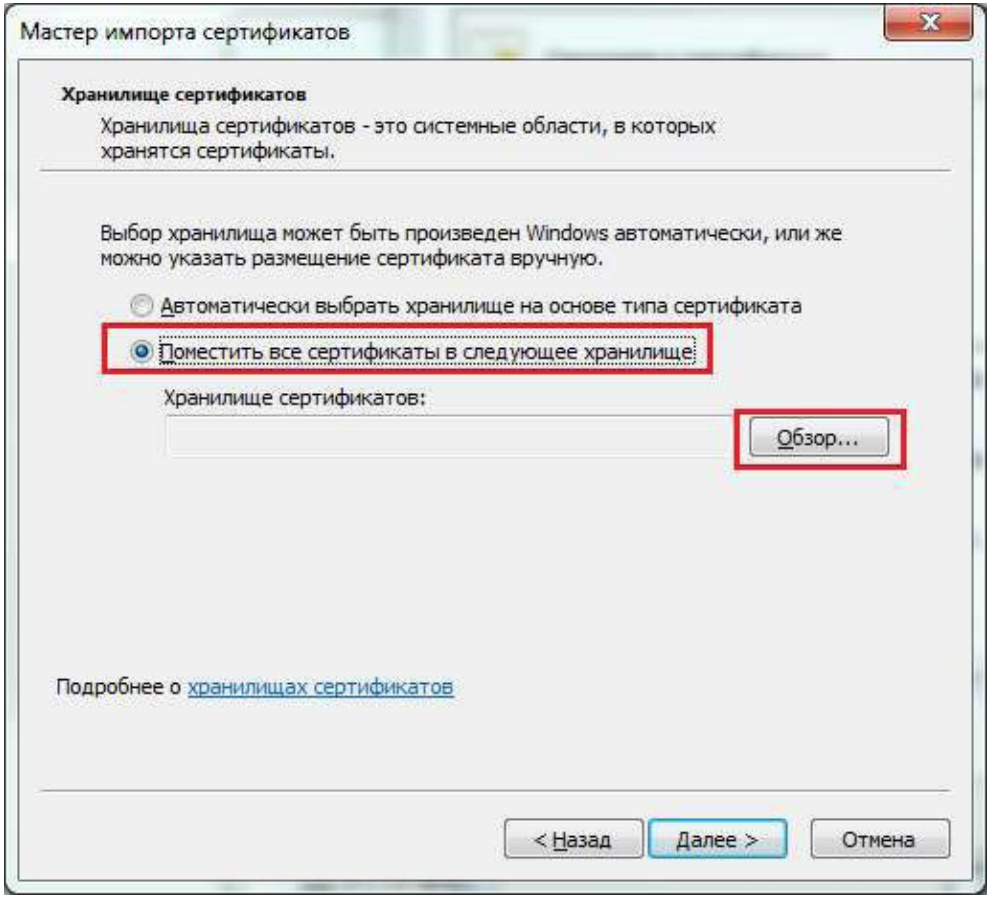

Рисунок . Выбор хранилища сертификата.

Шаг 6.3. Установка личного сертификата пользователя в хранилище «Личное» (при необходимости).

6. В окне выбора хранилища сертификатов выбрать контейнер «Личное».

7. Нажать кнопку «ОК».

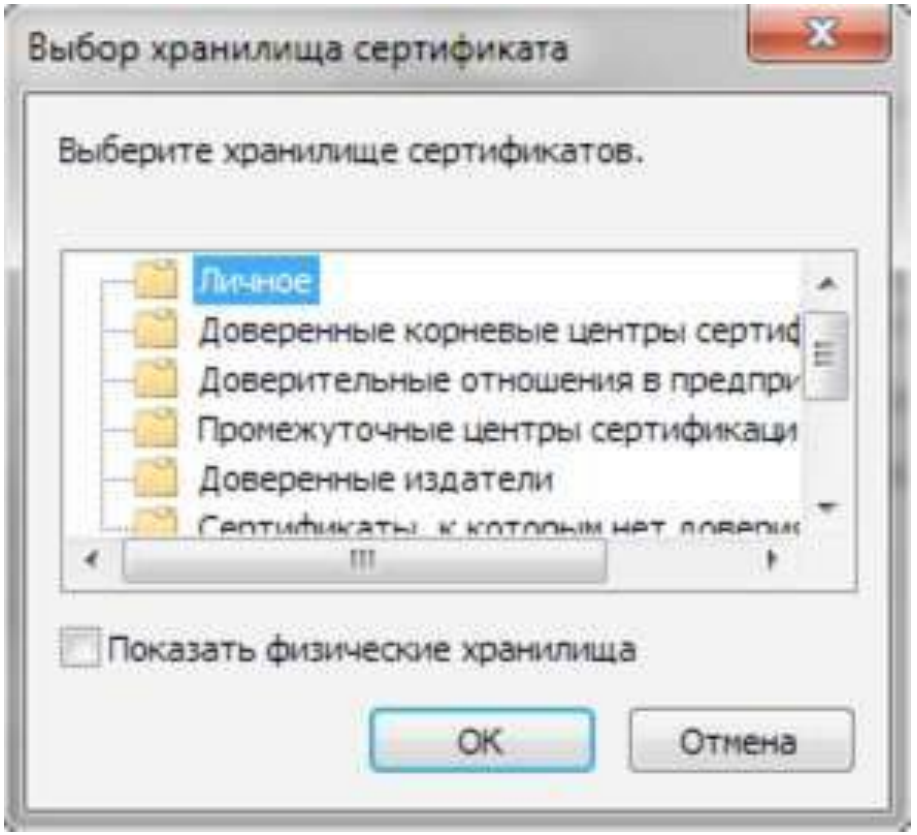

Рисунок . Выбор хранилища сертификата. Личное.

Шаг 6.4. Установка личного сертификата пользователя в хранилище «Личное» (при необходимости).

8. Нажать кнопку «Далее>».

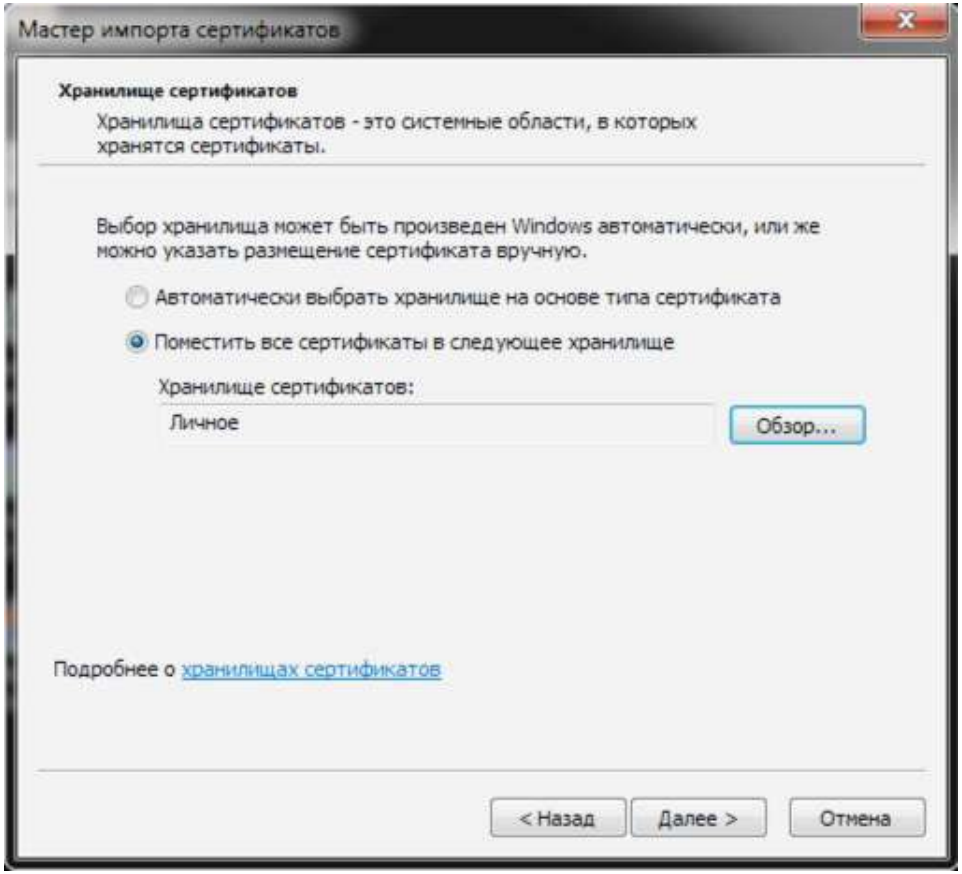

Рисунок . Выбор хранилища сертификата. Установка.

Шаг 6.5. Установка личного сертификата пользователя в хранилище «Личное» (при необходимости).

9. Нажать кнопку «Готово».

10. В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен».

11. Нажать кнопку «ОК».

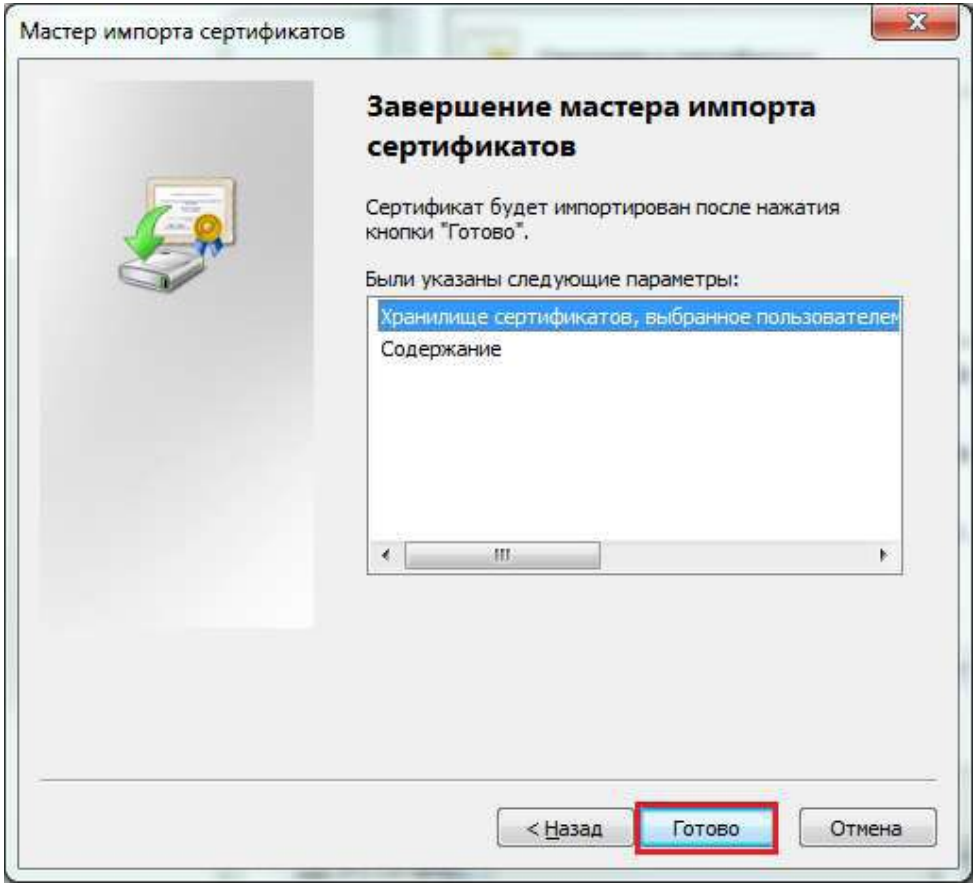

Рисунок . Завершение установки.

Шаг 7.1. Произвести вход в личный кабинет системы «Электронный бюджет».

1. Вставить ключевой носитель в USB разъем.

2. В веб-обозревателе перейти по адресу: **http://lk.budget.gov.ru/udu-webcenter**

3. На экране отобразится диалог выбора сертификата.

4. Выбрать хранилище сертификата (Сертификаты Windows) и в нем сертификат, который необходимо использовать для входа в личный кабинет.

5. Указать пароль доступа к ключевому носителю и нажать кнопку «ОК».

6. В случае успешного входа, на экране отобразится главная страница личного кабинета пользователя системы «Электронный бюджет».

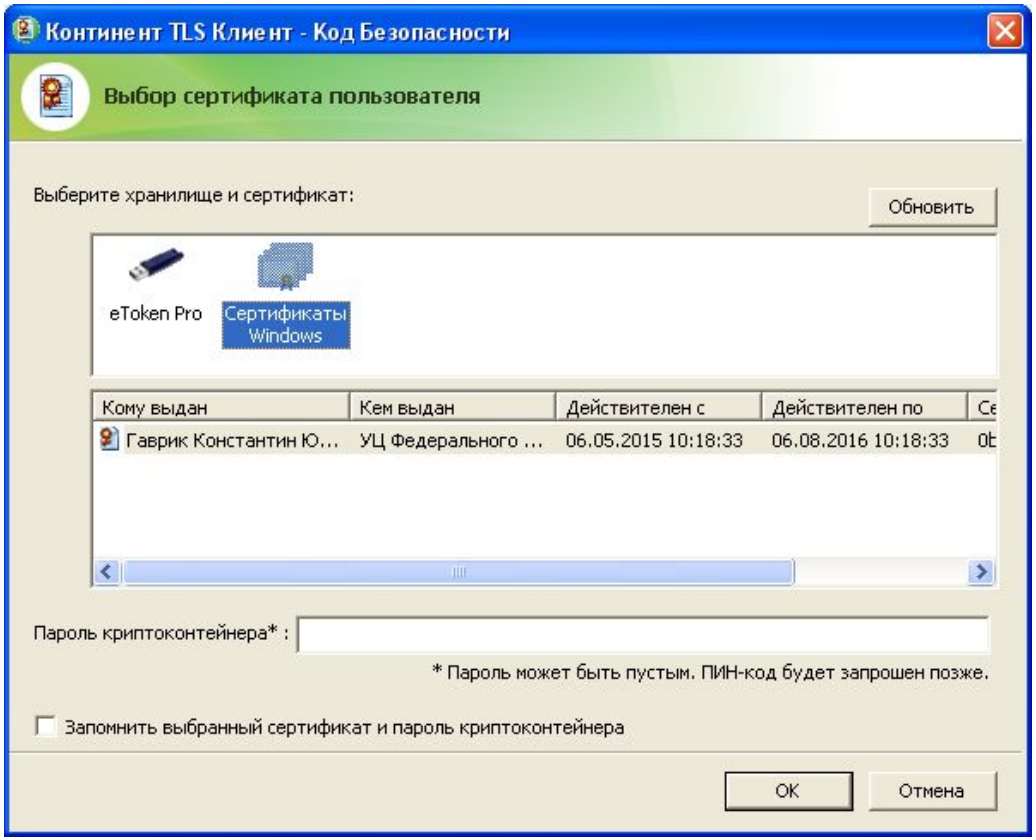

Рисунок. Выбор сертификата пользователя

Шаг 7.2. Произвести вход в личный кабинет системы «Электронный бюджет».

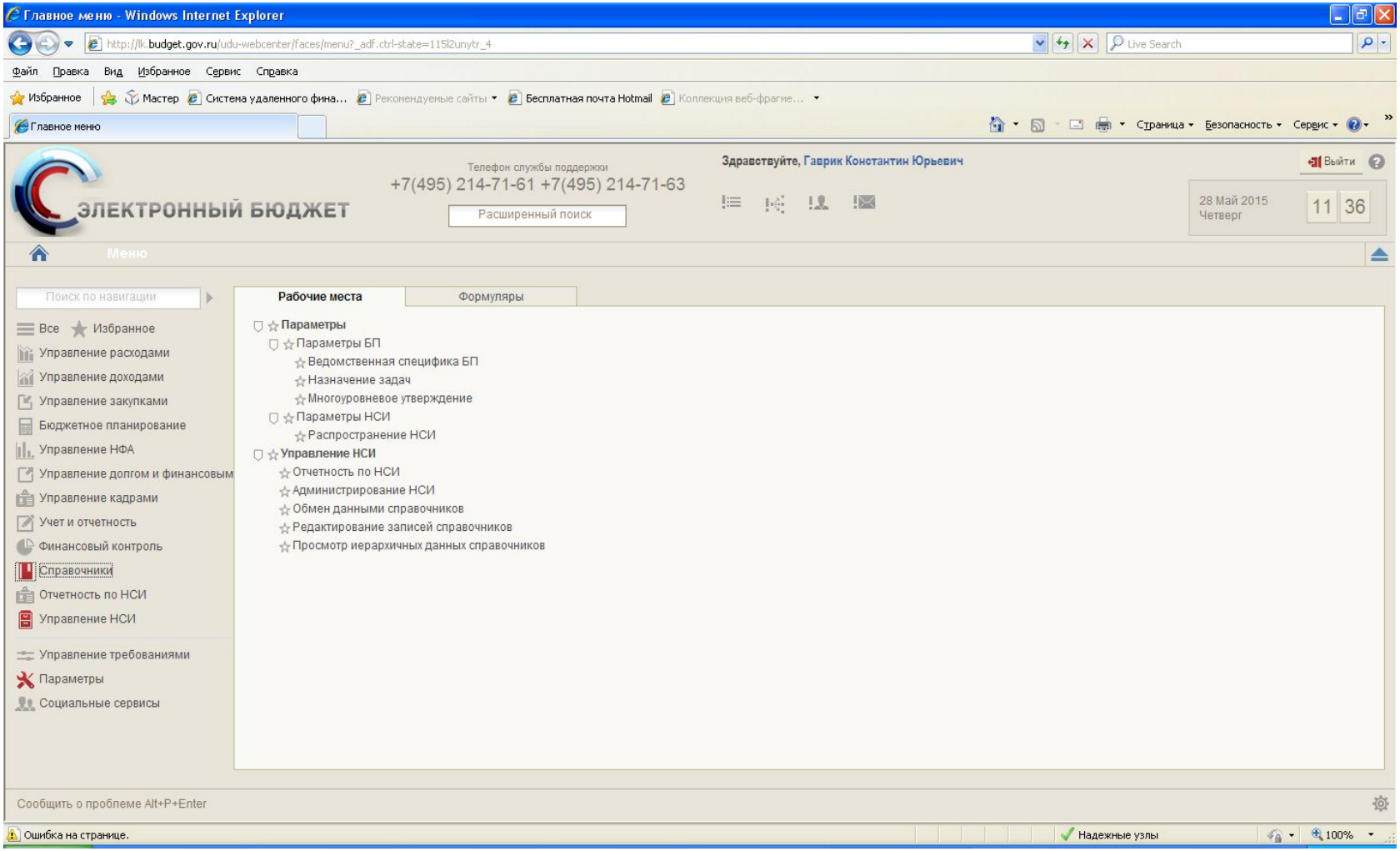

Рисунок. Личный кабинет пользователя