Приложение А
Требования к СКЗИ АРМ пользователя

На АРМ пользователя должны быть установлены:

1) Средства создания защищенного TLS-соединения:
   - СКЗИ «Континент TLS VPN Клиент» версии 1.2 или выше;

     Данное СКЗИ применяется только в том случае, если есть необходимость использования протокола HTTP и требуется возможность эксплуатации браузеров, не поддерживающих протокол HTTPS (с применением ГОСТ) с помощью СКЗИ «КриптоПро».
   - СКЗИ «КриптоПро CSP» версии 4.0 или выше;

     Для КриптоПро CSP следует установить СКЗИ «КриптоПро ЭЦП Browser plug-in».
2) Средства ЭП: СКЗИ «Jinn-Client» версии 1.0.3050.0 или выше;
3) Корневой сертификат Минкомсвязи и промежуточный сертификат УЦ ФК.

А.1 Требуемые ОС и носители ключевой информации сертификата пользователя

А.1.1 СКЗИ «Континент TLS VPN Клиент»

1) СКЗИ «Континент TLS VPN Клиент» поддерживает следующие носители ключевой информации сертификата пользователя:
   - USB-флеш-накопители;
   - USB-ключи: Рутокен, Рутокен Lite, Рутокен S (версия 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ;
   - смарт-карты: Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), eToken PRO, Esmart, Esmart ГОСТ;
   - идентификаторы DS1995, DS1996.
2) СКЗИ «Континент TLS VPN Клиент» работает на следующих ОС семейства Windows:

— MS Windows 10;

— MS Windows 8;

— MS Windows 7;

— MS Windows Vista;

— MS Windows XP.

Подробная информация о поддерживаемых ОС содержится в формулярах соответствующих версий СКЗИ «Континент TLS VPN Клиент».

А.1.2 СКЗИ «КриптоПро CSP»

1) Перечень поддерживаемых носителей приведен в фомуляре «КриптоПро CSP».
2) СКЗИ «КриптоПро CSP» (только сертифицированные версии) работает на следующих ОС семейства Windows:
   — MS Windows 10 (x86/x64);
   — MS Windows 8 (x86/x64). Поддерживает «КриптоПро CSP» только с версией 4.0;
   — MS Windows 7 (x86/x64);

Наиболее полная информация о поддерживаемых ОС содержится в формулярах соответствующих версий СКЗИ «КриптоПро CSP» и СКЗИ «КриптоПро ЭЦП Browser plug-in».

Приложение Б
Установка и настройка СКЗИ АРМ пользователя

Б.1 Порядок подготовки СКЗИ АРМ

Установка и настройка СКЗИ АРМ пользователя должна выполняться под учетной записью пользователя, входящего в группу локальных администраторов.

Порядок подготовки АРМ пользователя приведен ниже в таблице.

Таблица 4 – Порядок подготовки АРМ пользователя

Операция	Раздел
Проверка соответствия характеристик АРМ требованиям, приведенным в подразделе 3.1 и приложении Б настоящего документа.	Б.2.1
Копирование сертификатов сервера TLS в локальную директорию АРМ пользователя.	Б.2.2
Копирование сертификатов ГУЦ и сертификатов УЦ Федерального казначейства в локальную директорию АРМ пользователя.	Б.2.3
Установка сертификатов ГУЦ в локальное хранилище компьютера.	Б.2.4
Установка корневых сертификатов УЦ Федерального казначейства в локальное хранилище компьютера.	Б.2.5
Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя (при необходимости).	Б.2.6
Установка криптопровайдера КриптоПРО CSP.	Б.2.7
Установка КриптоПро ЭЦП Browser plug-in.	Б.2.8
Установка драйвера используемого носителя ключевой информации.	Б.2.9
Установка СКЗИ «Jinn-client».	Б.2.10
Установка и настройка СКЗИ «Континент TLS VPN Клиент».	Б.2.11
Установка опционального ПО «eXtended Container» (требуется для подписи посредством СКЗИ «Jinn-client» с сертификатами ГОСТ Р 34.10-2012).	Б.2.12
Установка Jinn Sign Extension Provider.	Б.2.13
Установка расширения Jinn Sign Extension.	Б.2.14

Б.2 Описание операций по настройке СКЗИ АРМ

Б.2.1 Проверка характеристик АРМ

Перед началом настройки АРМ пользователя подсистемы следует убедиться, что АРМ соответствует требованиям, приведенным в подразделе 3.1 и приложении Б настоящего документа.

Порядок установки программного обеспечения и расширений должен быть произведен в соответствии с пунктами, приведенными в подразделе 3.2 и текущем приложении.

Б.2.2 Копирование сертификатов сервера TLS

Для копирования файлов сертификатов сервера TLS в локальную директорию АРМ пользователя необходимо:

1) Скачать сертификат сервера TLS с официального сайта Федерального казначейства: www.roskazna.ru.
2) Выгрузить из инструкции сертификат сервера TLS в локальную директорию АРМ пользователя, в которую необходимо сохранить файл.

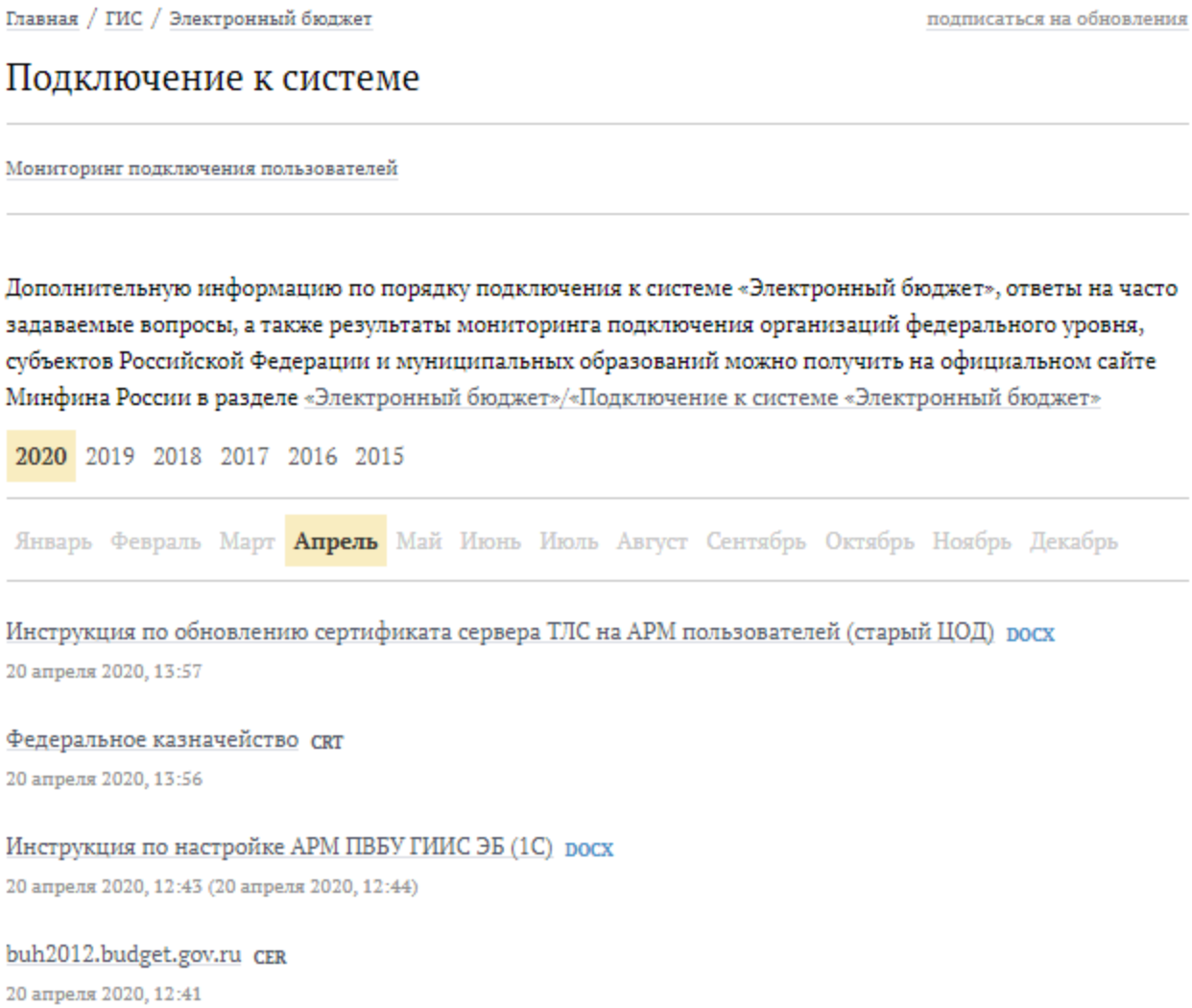


Рисунок 97 – Инструкция по обновлению сертификата TLS

Б.2.3 Копирование сертификатов ГУЦ и сертификатов УЦ Федерального казначейства

Для копирования файлов сертификатов ГУЦ и УЦ Федерального казначейства в локальную директорию АРМ пользователя необходимо:

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

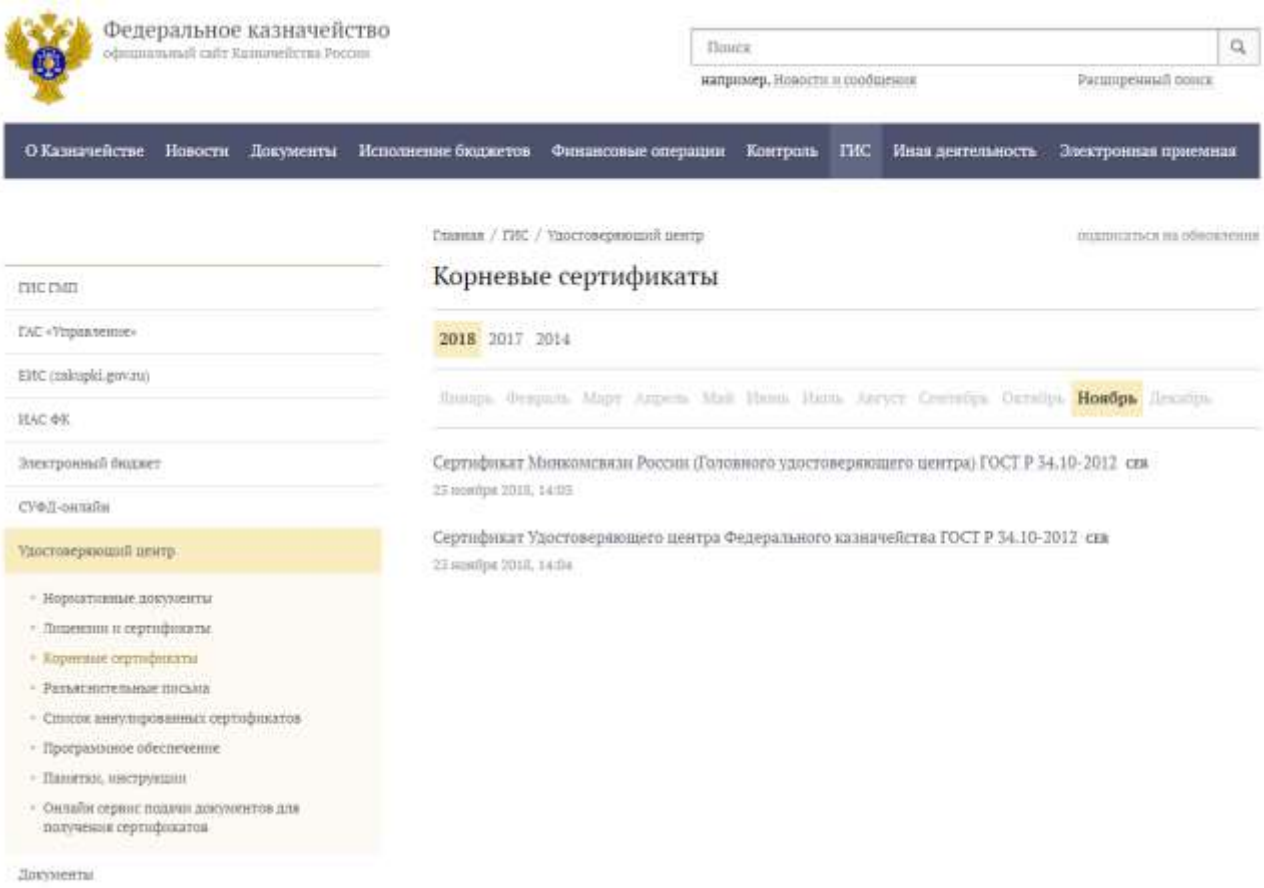


Рисунок 98 – Опубликованные сертификаты УЦ

2) Перейти в раздел ГИС > Удостоверяющий центр > Корневые сертификаты (рисунок выше).

3) Активировать ссылку на скачивание сертификатов в зависимости от требуемого ГОСТ.

   Ссылка на скачивание сертификата ГУЦ по ГОСТ Р 34.10-2012: http://www.roskazna.ru/upload/iblock/7e3/guts_2012.cer.

   Ссылка на скачивание корневого сертификата Удостоверяющего центра Федерального казначейства по ГОСТ Р 34.10-2012: http://www.roskazna.ru/upload/iblock/acb/fk_2012.cer.

   Ссылка на скачивание корневого сертификата Удостоверяющего центра Федерального казначейства по ГОСТ Р 34.10-2012:

   http://www.roskazna.ru/upload/iblock/024/uts-fk_2020.cer

4) На предложение сохранить файл сертификата выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.

5) Сохранить файл сертификата.

Б.2.4 Установка сертификатов ГУЦ в локальное хранилище компьютера

Для установки сертификатов ГУЦ в хранилище сертификатов компьютера средствами операционной системы семейства Windows необходимо:

1) Через контекстное меню файла сертификата ГУЦ выбрать пункт меню «Установить сертификат».
2) На экране отобразится мастер импорта сертификатов (рисунок ниже).

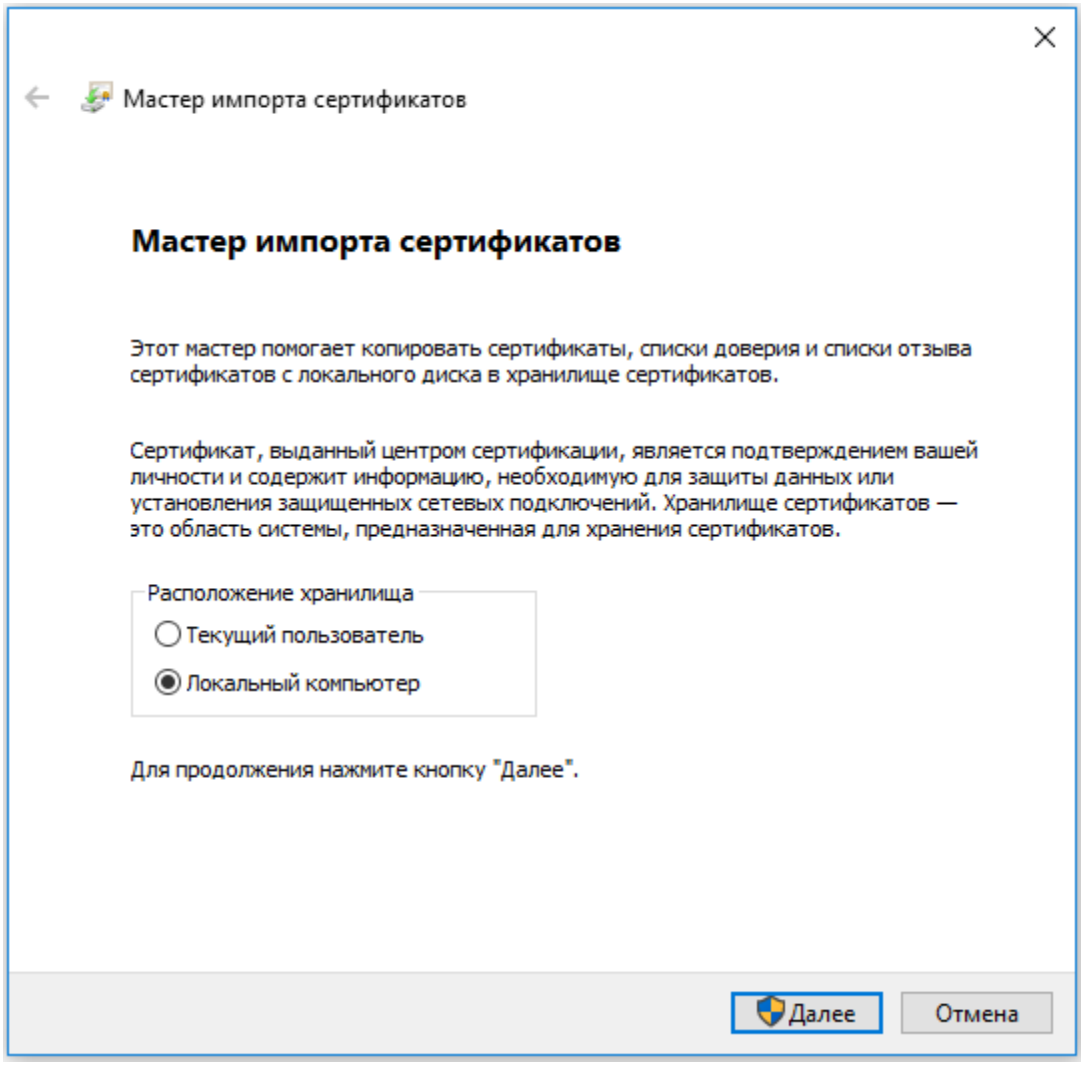


Рисунок 99 – Мастер импорта сертификатов

3) Выбрать хранилище «Локальный компьютер» и нажать кнопку «Далее».

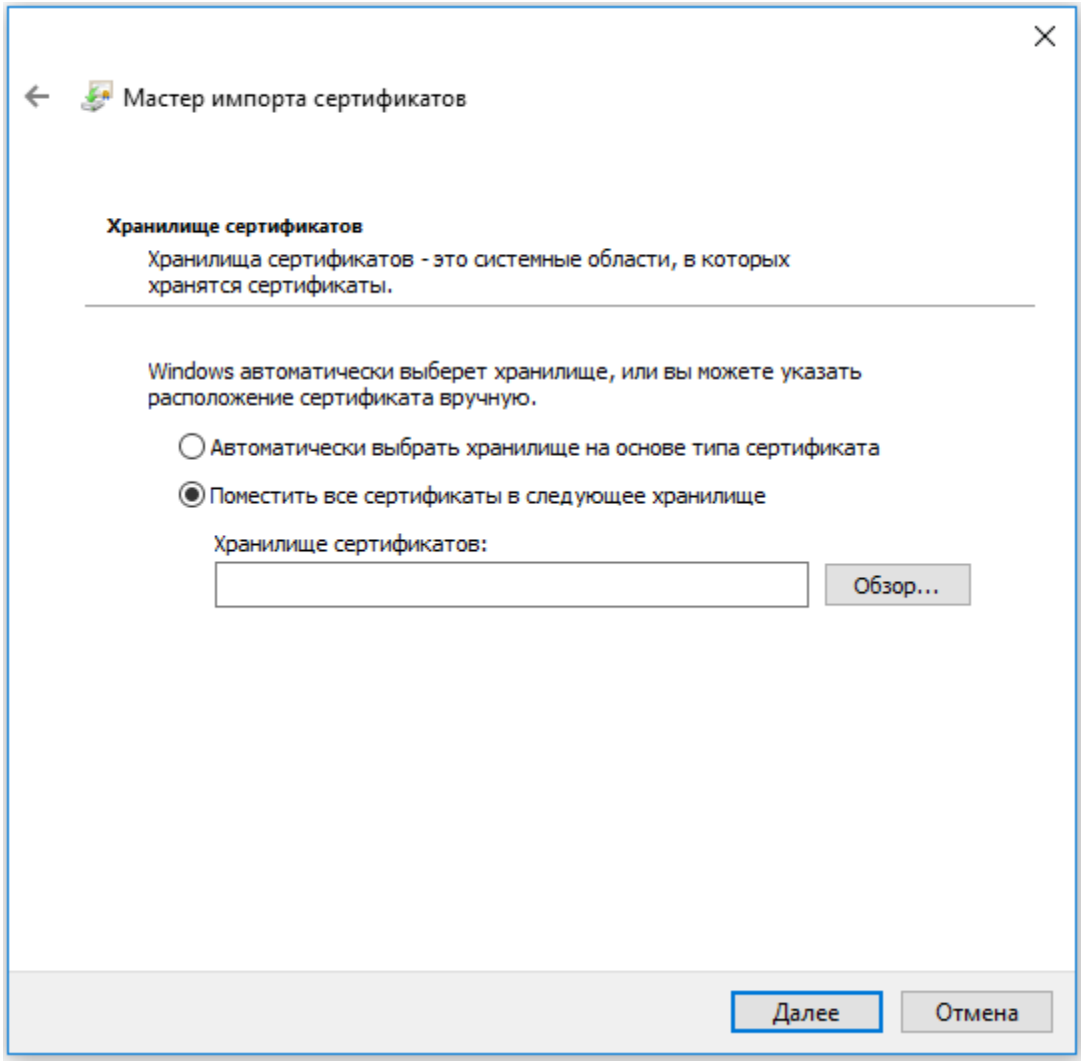


Рисунок 100 – Выбор хранилища сертификата

4) В окне «Хранилище сертификата» (Рисунок 100) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».

5) Нажать кнопку «Обзор…». Откроется окно «Выбор хранилища сертификата» (Рисунок 101).

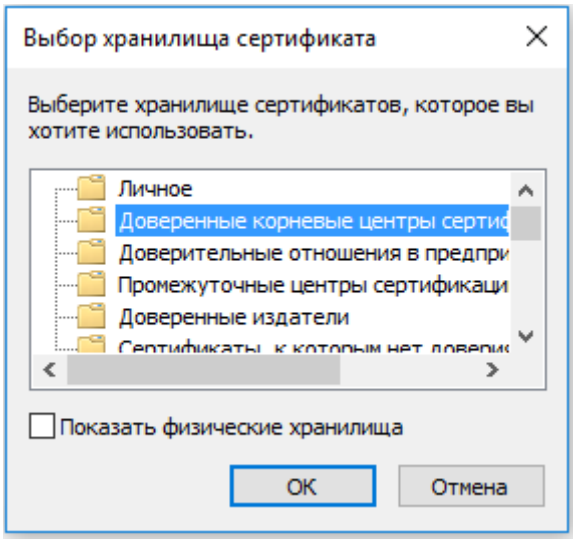


Рисунок 101 – Выбор хранилища сертификата

6) Выбрать хранилище «Доверенные корневые центры сертификации», нажать кнопку «ОК».

   Откроется окно завершения работы мастера импорта сертификатов (Рисунок 102).

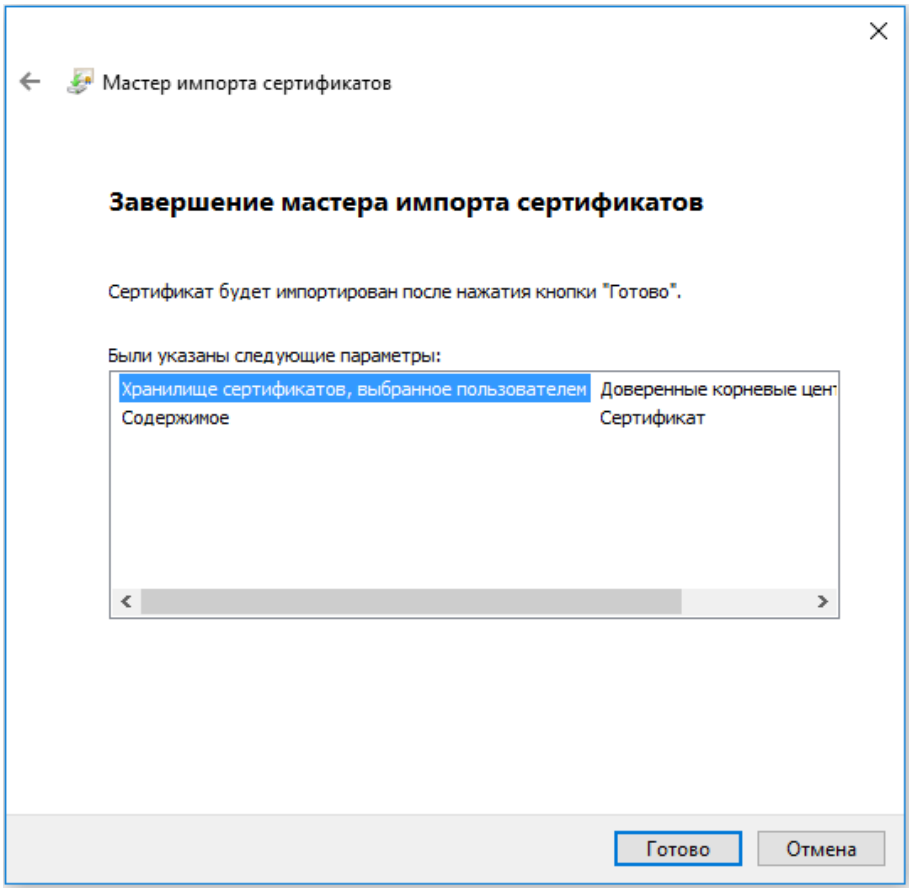


Рисунок 102 – Окно завершения работы мастера импорта сертификатов

7) Нажать кнопку «Готово».

   Появится сообщение, что импорт успешно выполнен (Рисунок 103).

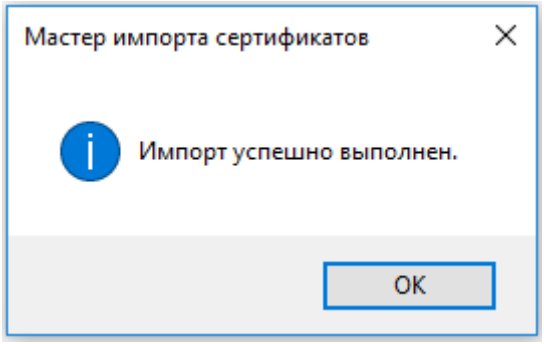


Рисунок 103 – Завершение установки

8) Нажать кнопку «ОК».

Примечание – Если на шаге 3 данной инструкции отсутствует возможность выбора хранилища Локального компьютера, следует обратиться к системному администратору ЛВС для выполнения операции с правами локального администратора АРМ.

Б.2.5 Установка корневых сертификатов УЦ Федерального казначейства в локальное хранилище компьютера

Необходимо установить два подчиненных корневых сертификата УЦ ФК.

Для установки корневого корневых сертификатов УЦ ФК в хранилище сертификатов компьютера средствами операционной системы семейства Windows необходимо:

1) Через контекстное меню файла корневого сертификата УЦ Федерального казначейства выбрать пункт меню «Установить сертификат».

   На экране отобразится мастер импорта сертификатов (Рисунок 104).

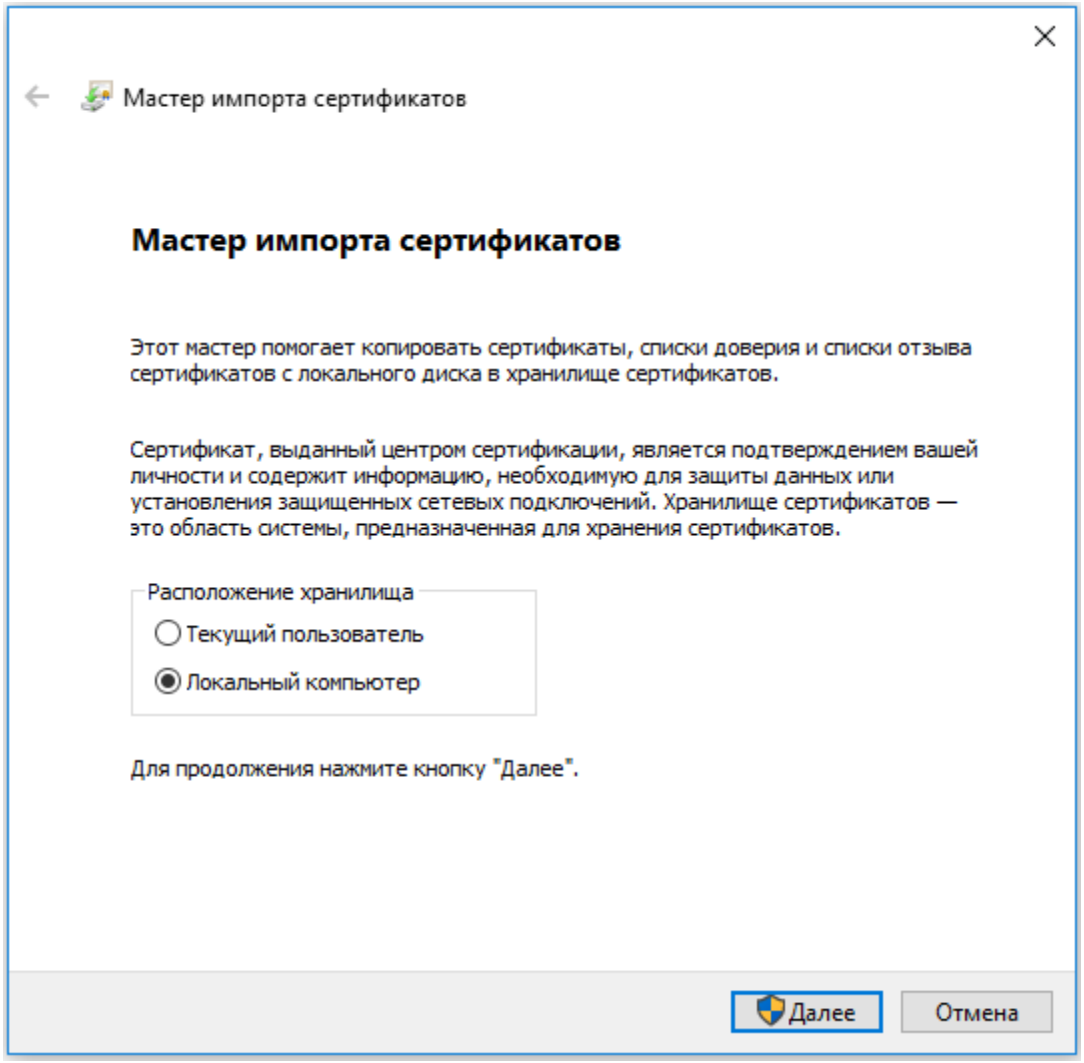


Рисунок 104 – Мастер импорта сертификатов

2) Выбрать хранилище «Локальный компьютер» и нажать кнопку «Далее».

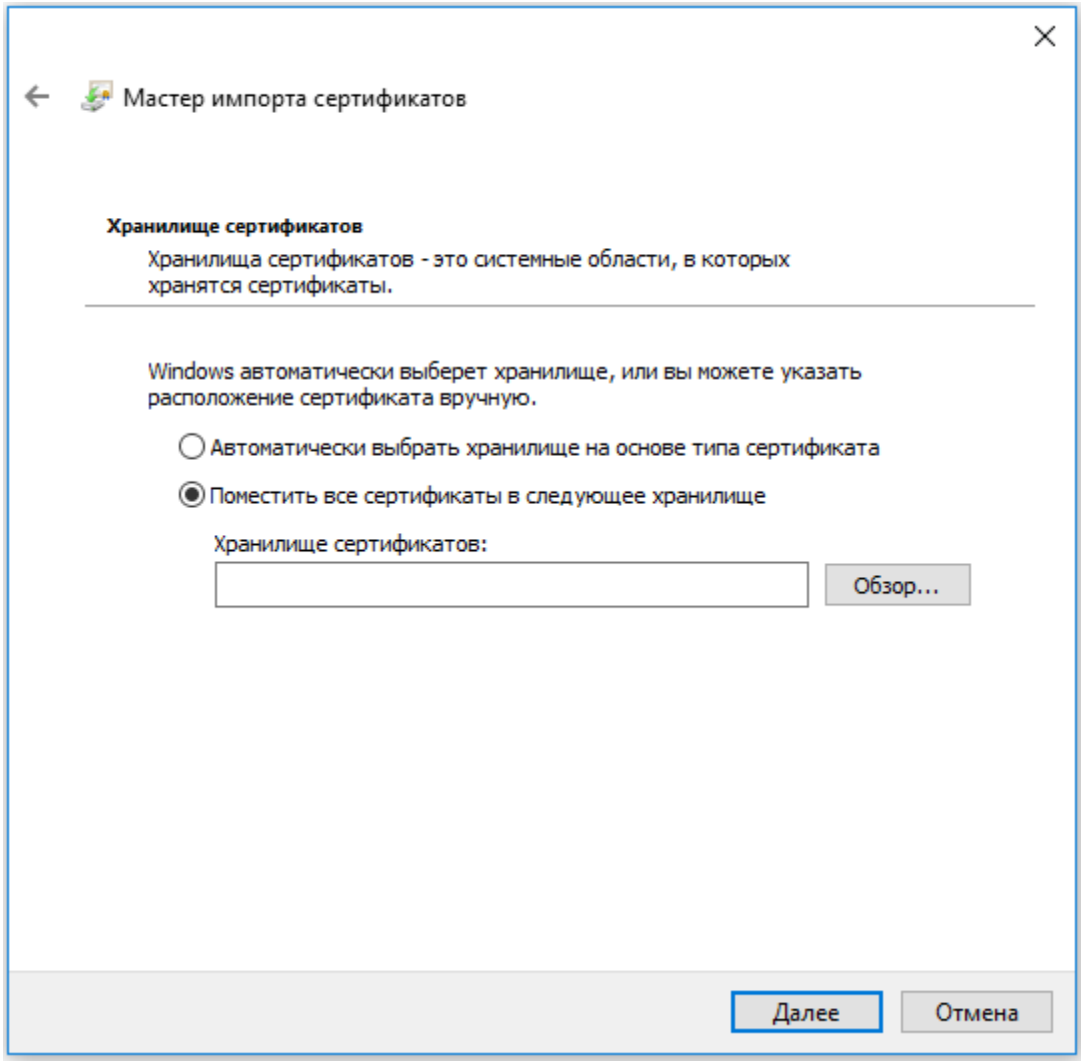


Рисунок 105 – Выбор хранилища сертификата

3) В окне «Хранилище сертификата» (Рисунок 105) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».
4) Нажать кнопку «Обзор…». Откроется окно «Выбор хранилища сертификата» (Рисунок 106).

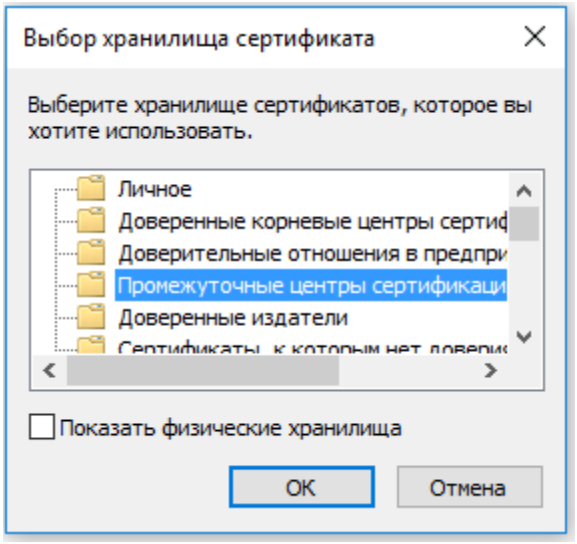


Рисунок 106 – Выбор хранилища сертификата

5) Выбрать хранилище «Промежуточные центры сертификации», нажать кнопку «ОК».

   Откроется окно завершения работы мастера импорта сертификатов (Рисунок 107).

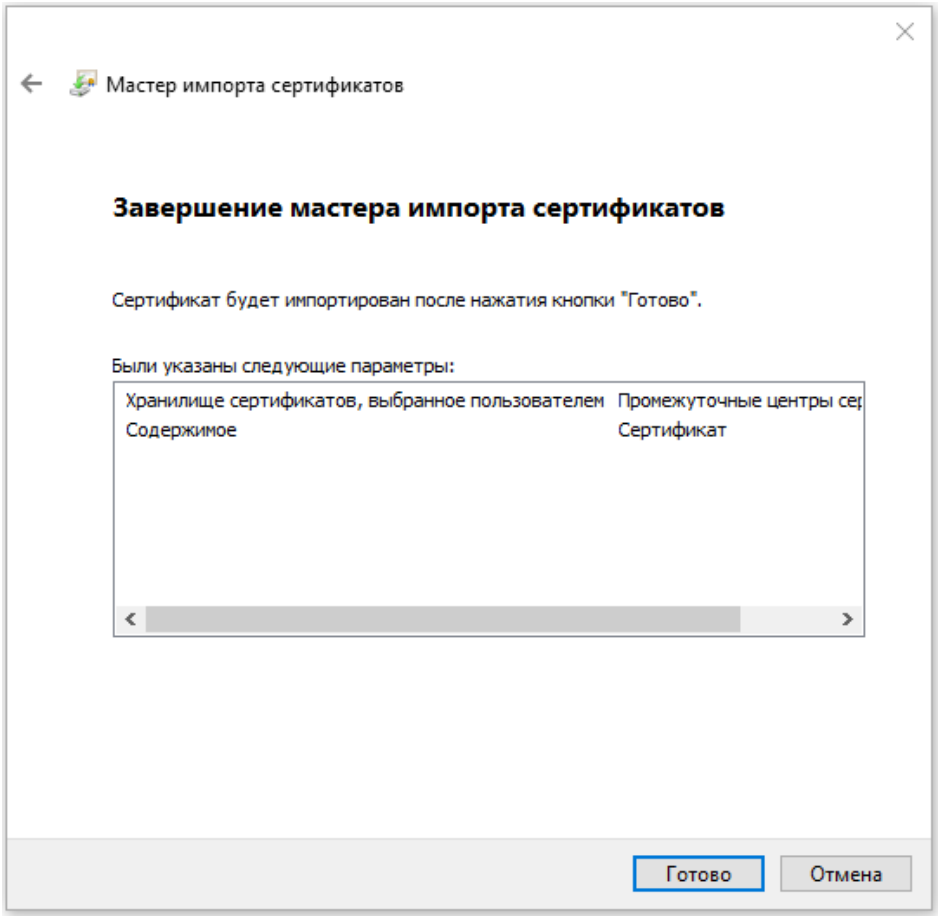


Рисунок 107 – Окно завершения работы мастера импорта сертификатов

6) Нажать кнопку «Готово».

Появится сообщение, что импорт успешно выполнен.

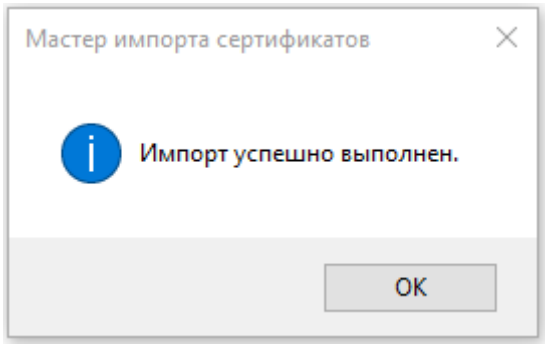


Рисунок 108 – Завершение установки

7) Нажать кнопку «ОК».

Примечание – Если на шаге 3 данной инструкции отсутствует возможность выбора хранилища Локального компьютера, следует обратиться к системному администратору ЛВС для выполнения операции с правами локального администратора АРМ.

Б.2.6 Установка сертификата пользователя в хранилище личных сертификатов АРМ (при необходимости)

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется в случае, если файл сертификата пользователя не является единым целым с закрытым ключом (в процессе получения в УЦ сертификат в формате «*.cer» был записан на отдельный носитель информации).

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в подсистему.

Для установки сертификата пользователя в хранилище личных сертификатов АРМ пользователя средствами СКЗИ «КриптоПро» необходимо:

1) Открыть приложение «КриптоПро CSP» и перейти на вкладку «Сервис»;

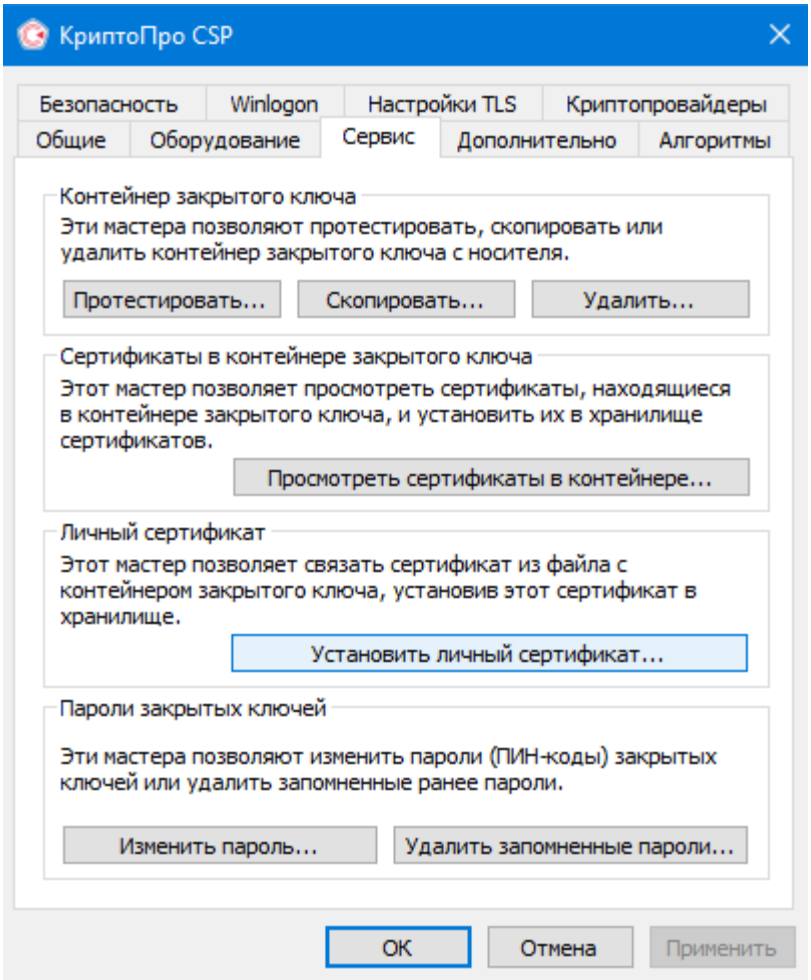


Рисунок 109 – Вкладка «Сервис»

2) Нажать кнопку «Установить личный сертификат»;

3) Выбрать личный сертификат, нажав на кнопку «Обзор»;

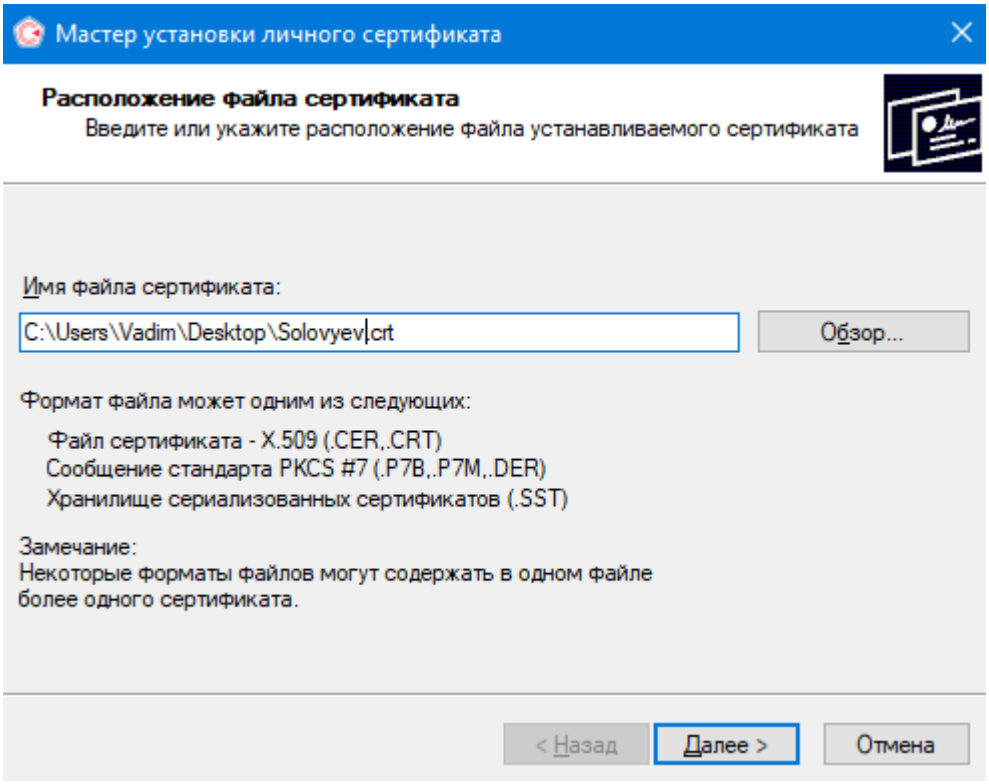


Рисунок 110 – Выбор сертификата

4) Нажать кнопку «Далее»;
5) Отобразится окно с данными о выбранном сертификате;
6) Нажать кнопку «Далее»;
7) Указать контейнер закрытого ключа;

   Если контейнер располагается на присоединенном носителе, то следует установить признак «Найти контейнер автоматически».

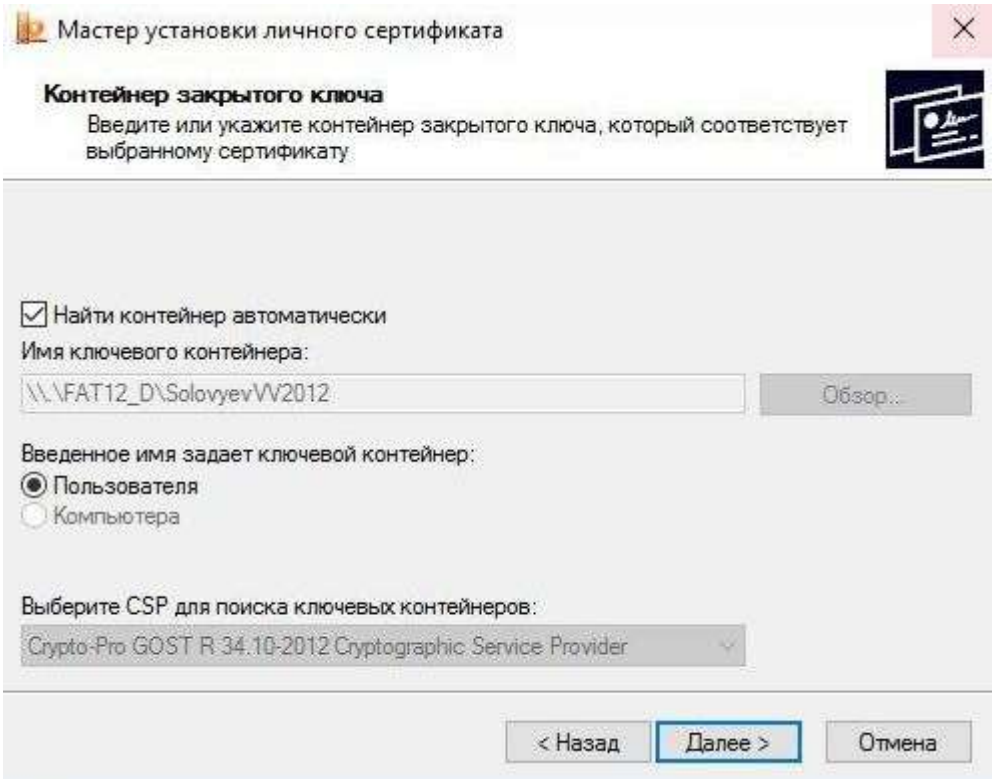


Рисунок 111 – Выбор контейнера закрытого ключа

8) Указать хранилище сертификата;

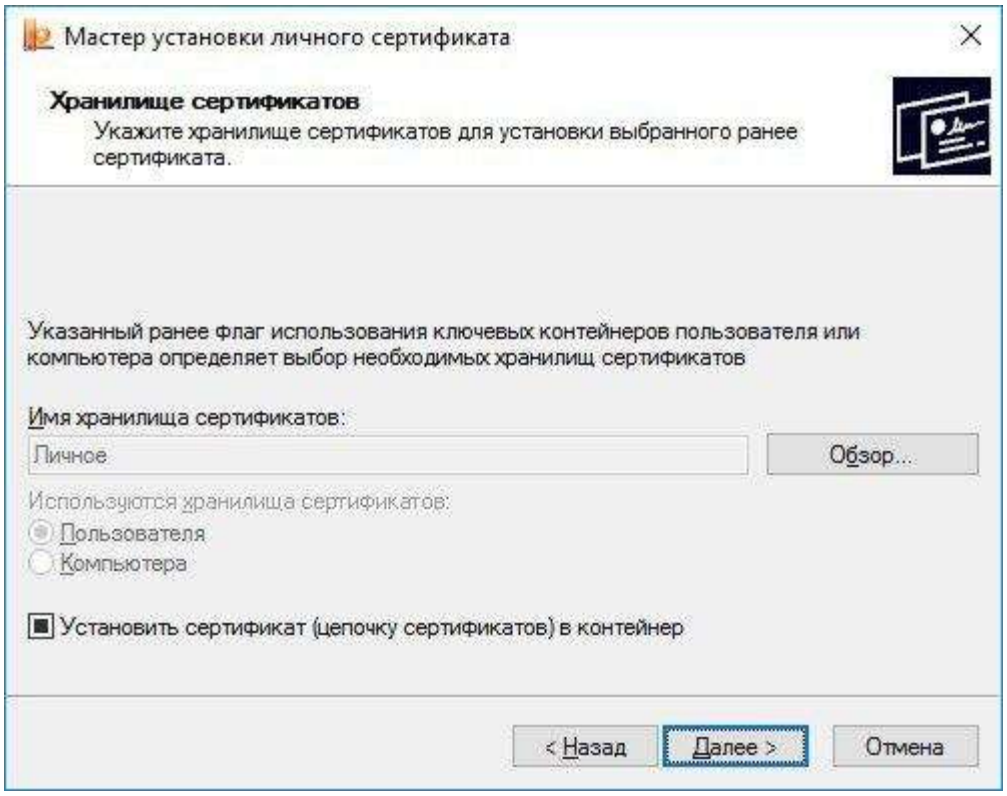


Рисунок 112 – Выбор хранилища сертификата

9) Нажать кнопку «Готово»;

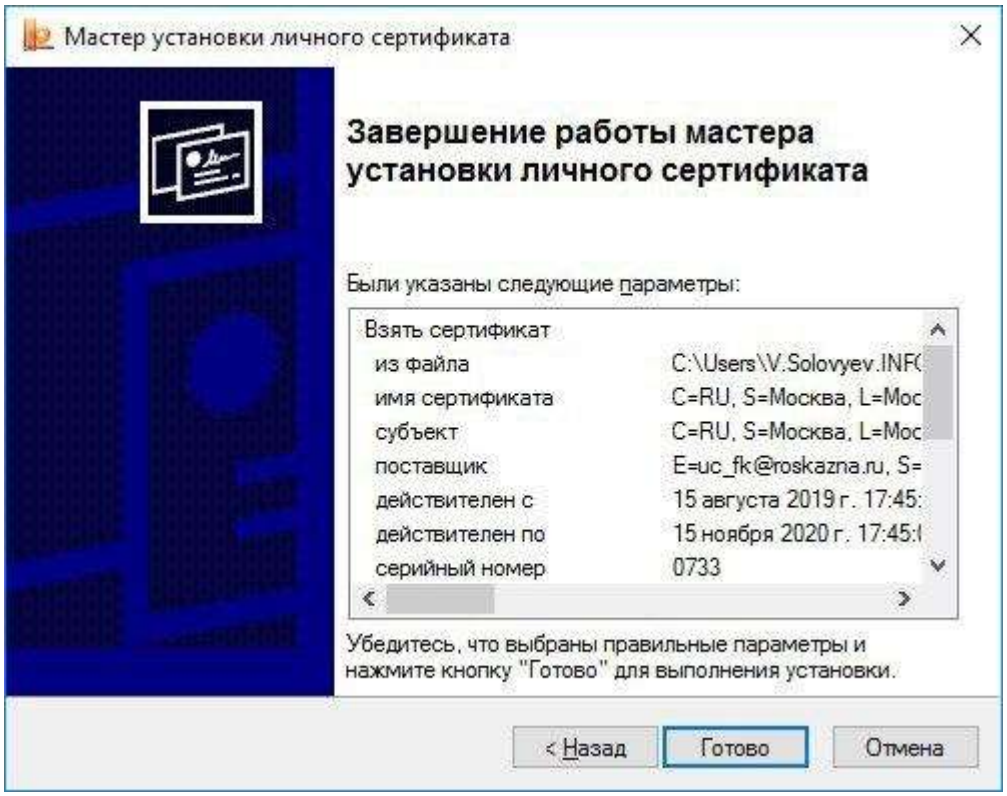


Рисунок 113 – Завершение настроек установки сертификата

10) Сертификат установлен в контейнер закрытого ключа и в хранилище «Личное» на АРМ пользователя.

Б.2.7 Установка и настройка криптопровайдера КриптоПро CSP

Установка СКЗИ «КриптоПро» обязательна.

В случае отсутствия дистрибутива необходимо обратиться в территориальный орган Федерального казначейства по месту нахождения. Также можно просмотреть порядок получения дистрибутивов на интернет-сайтах Управлений ФК в разделе ГИС > Удостоверяющий центр.

Для установки криптопровайдера КриптоПро CSP необходимо:

1) Запустить файл установки КриптоПро CSP. Откроется стартовое окно мастера установки КриптоПро CSP.

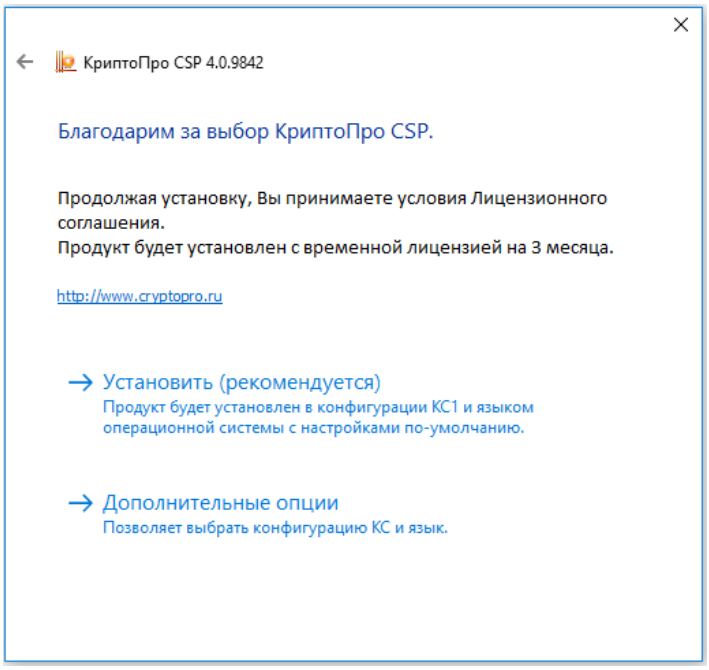


Рисунок 114 – Стартовое окно мастера установки КриптоПро CSP

2) Нажать кнопку «Установить (рекомендуется)».

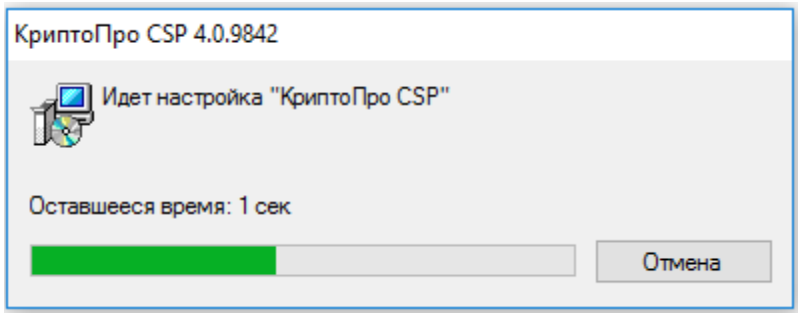


Рисунок 115 – Процесс установки КриптоПро CSP

3) Отобразится окно процесса установки КриптоПро CSP (Рисунок 115).

   После успешной установки криптопровайдера отобразится диалог «КриптоПро CSP успешно установлен» (Рисунок 116).

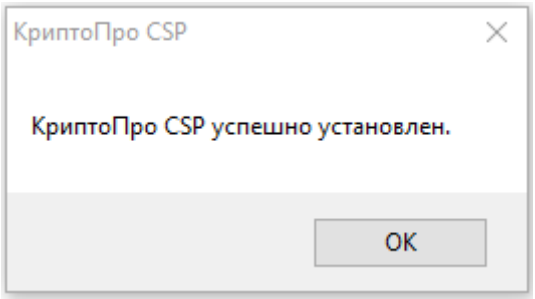


Рисунок 116 – Успешная установка КриптоПро CSP

4) Нажать кнопку «ОК».

5) Запустить КриптоПро CSP. Во вкладке общие нажать кнопку «Ввод лицензии» и ввести лицензионный ключ (Рисунок 117).

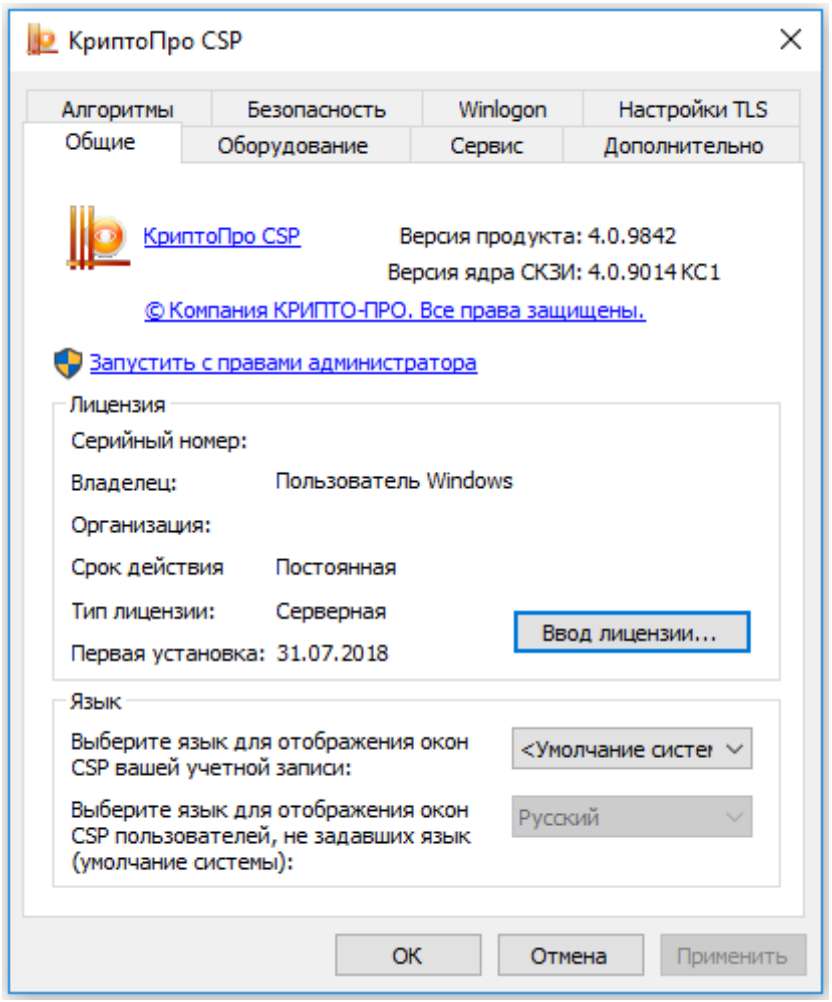


Рисунок 117 – Вкладка «Общие». КриптоПро CSP

Для настройки криптопровайдера необходимо выполнить следующие действия:

1) Запустить КриптоПро CSP от имени Администратора.
2) Перейти на вкладку «Настройки TLS».
3) Отметить в разделе «Клиент» следующие чекбоксы (Рисунок 118):
   - Не проверять сертификат сертификат сервера на отзыв;
   - Не проверять назначение собственного сертификата.

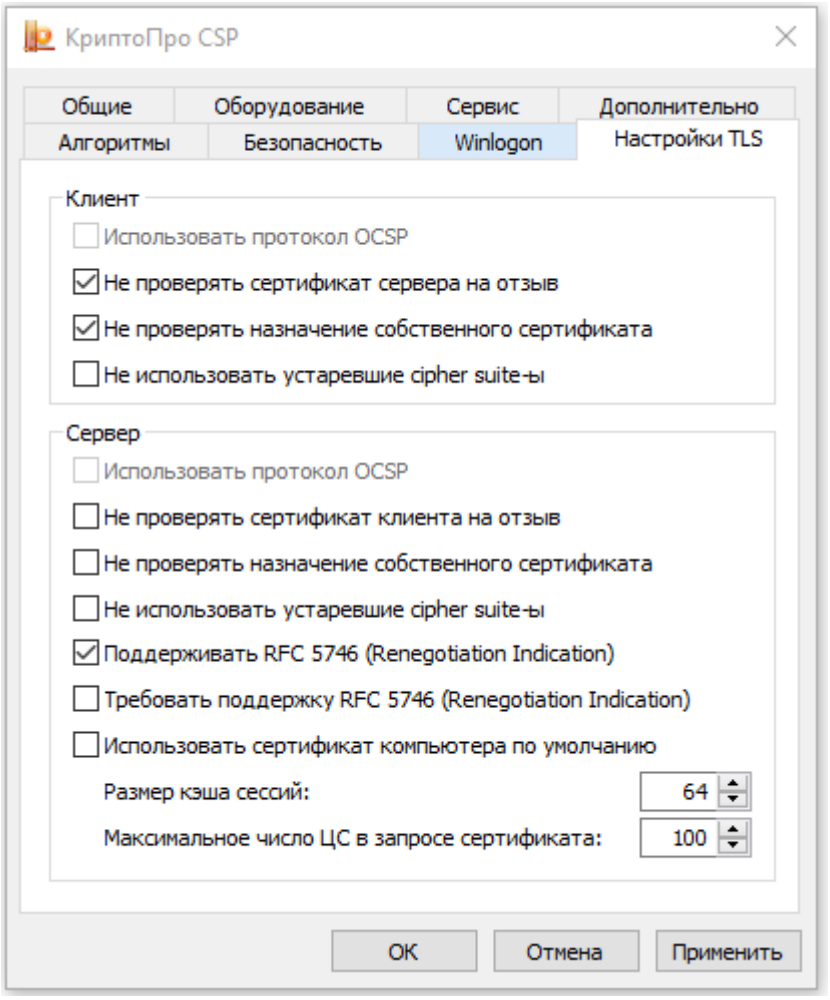


Рисунок 118 – Вкладка «Настройки TLS». КриптоПро CSP

4) Нажать кнопку «Применить». Появится запрос на перезагрузку АРМ.

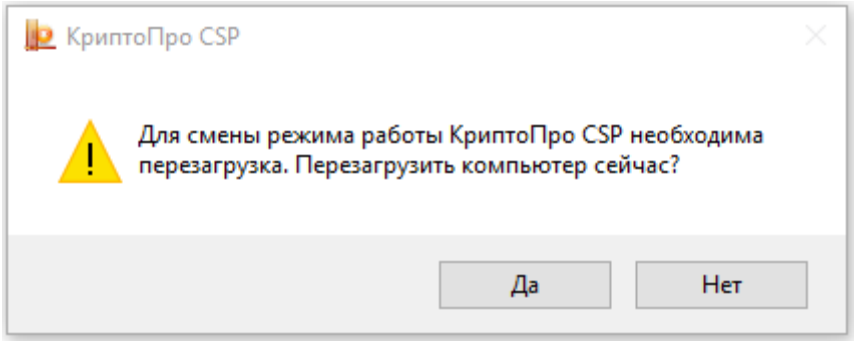


Рисунок 119 – Запрос на перезагрузку после смены режима работы

5) Нажать кнопку «Да».
6) АРМ перезагрузится.

Б.2.8 Установка КриптоПро ЭЦП Browser plug-in

КриптоПро ЭЦП Browser plug-in версии 2.0 предназначен для создания и проверки электронной подписи на веб-страницах с использованием СКЗИ "КриптоПро CSP".

Файл установки доступен для скачивания по адресу: https://www.cryptopro.ru/products/cades/plugin/

Для установки КриптоПро ЭЦП Browser plug-in необходимо:

1) Запустить файл установки и в окне установки нажать кнопку «Да»
2) Дождаться окончания установки и нажать кнопку «ОК».

Б.2.9 Установка драйвера используемого носителя ключевой информации сертификата пользователя

Если в качестве носителя ключевой информации сертификата пользователя используется USB флеш-накопитель, установка драйвера данного накопителя осуществляется автоматически средствами ОС в момент первого использования данного накопителя.

Если в качестве носителя ключевой информации сертификата пользователя используется носитель типа eToken или Rutoken, необходимо выполнить установку драйвера соответствующего носителя на АРМ пользователя (если ранее не был установлен).

1) Если драйвер носителя типа Rutoken не установлен, то:
    a) Запустите программу-установщик драйвера Rutoken. Окно приветствия установщика драйверов Rutoken представлено на рисунке 120.

    При отсутствии программы-установщика драйвера необходимо обратиться к производителю носителя.

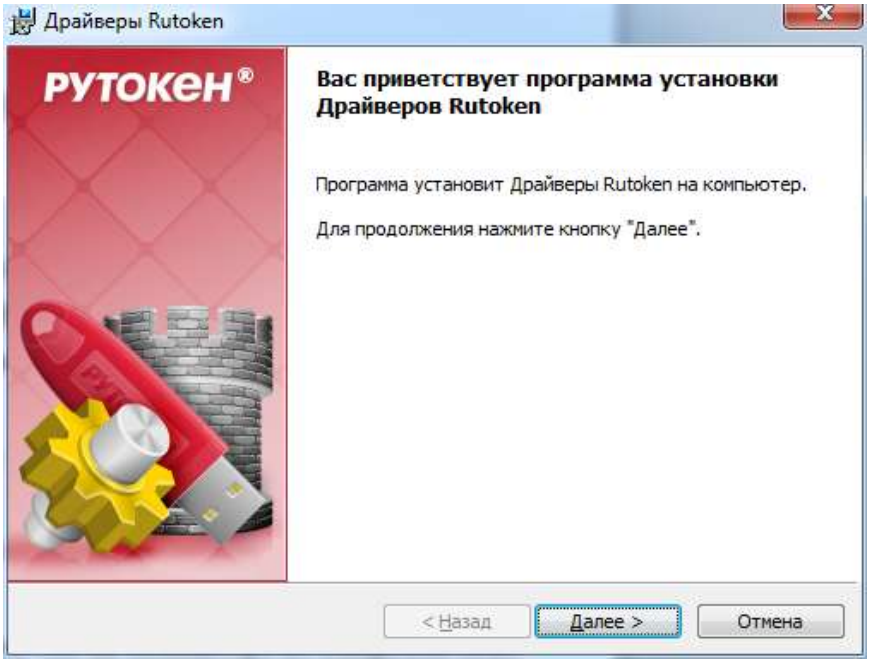


Рисунок 120 – Экранная форма приветствия установщика драйвера Rutoken

b) Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов (Рисунок 121).

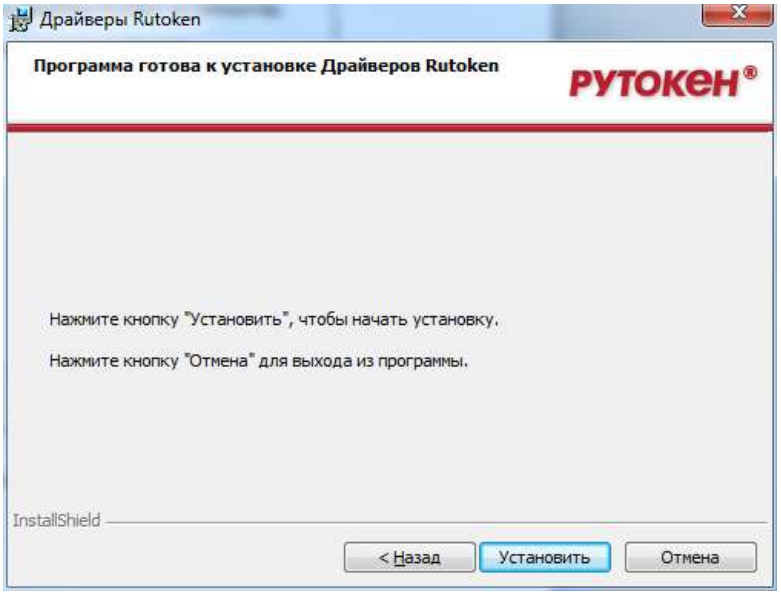


Рисунок 121 – Сообщение о готовности к выполнению установки драйверов

c) Нажмите кнопку «Установить». Начнется установка драйверов Rutoken на АРМ пользователя. Установка может занять несколько минут, информация о прогрессе установки выводится в окне, представленном на рисунке (Рисунок 122).

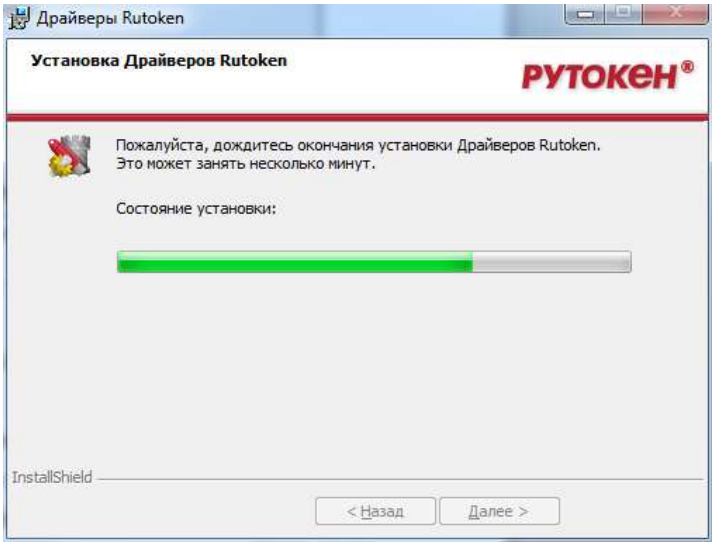


Рисунок 122 – Окно, информирующее о прогрессе установки драйверов Rutoken

d) После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 123).

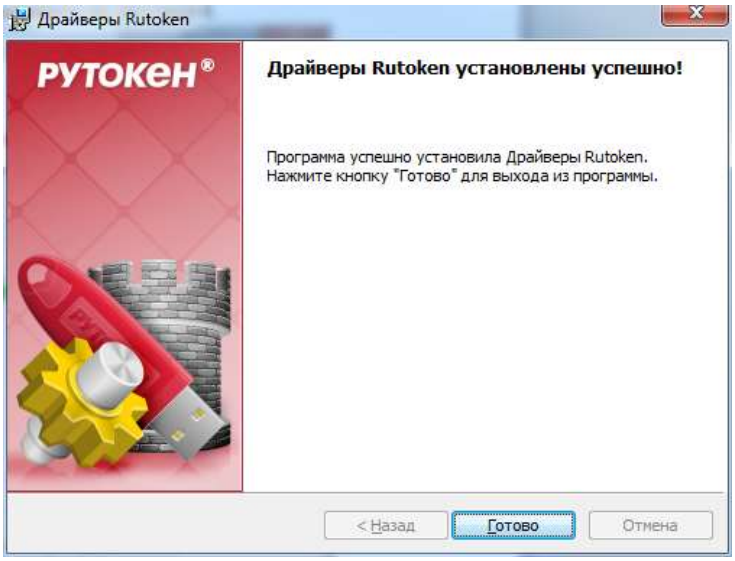


Рисунок 123 – Сообщение об успешной установке драйверов Rutoken

e) Нажмите кнопку «Готово». Окно установщика драйверов Rutoken будет закрыто.

f) В случае появления диалога о необходимости перезагрузки АРМ Пользователя, перезагрузить АРМ.

2) Если драйвер носителя типа eToken не установлен, то:

a) При отсутствии программы-установщика драйвера необходимо обратиться к производителю носителя.

b) Запустите программу-установщик драйвера eToken. Окно приветствия установщика драйвера eToken представлено на рисунке (Рисунок 124).

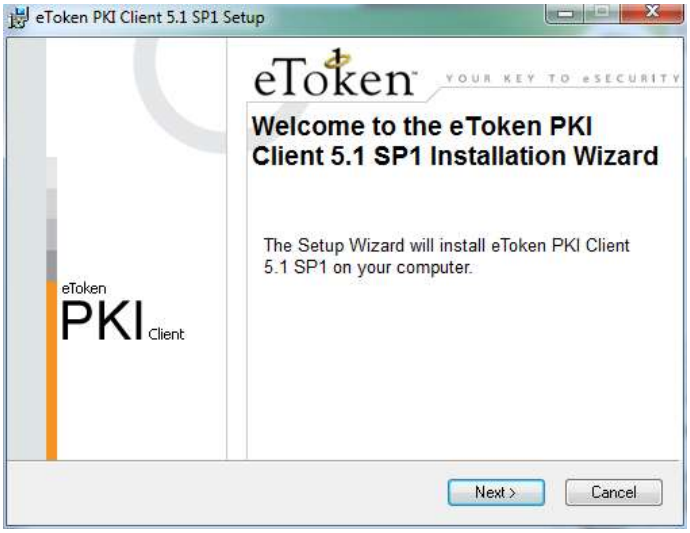


Рисунок 124 – Экранная форма приветствия установщика драйверов eToken

c) Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (Рисунок 125).



Рисунок 125 – Окно выбора языка программы, управляющей ключевыми носителями eToken

d) Так как для решения задач, возникающих при работе в подсистеме, данное ПО не будет применяться пользователями подсистемы, то выбор языка можно пропустить, нажав кнопку «Next». На экране появится диалог лицензионное соглашение (Рисунок 126).

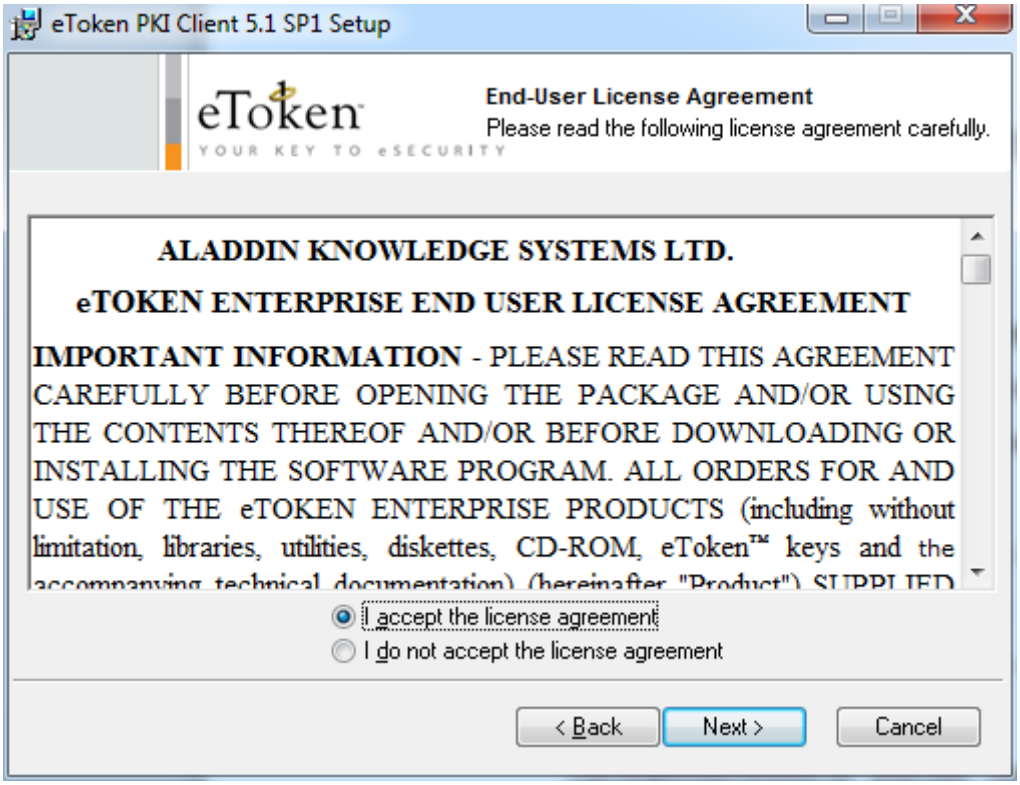


Рисунок 126 – Окно просмотра лицензионного соглашения

e) Выберите пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (Рисунок 127).



Рисунок 127 – Окно выбора пути для установки программы

f) Оставьте путь установки по умолчанию либо измените на необходимый. Нажмите кнопку «Next».

g) Начнется установка программы и драйверов. Диалог процесса установки представлен на рисунке (Рисунок 128).

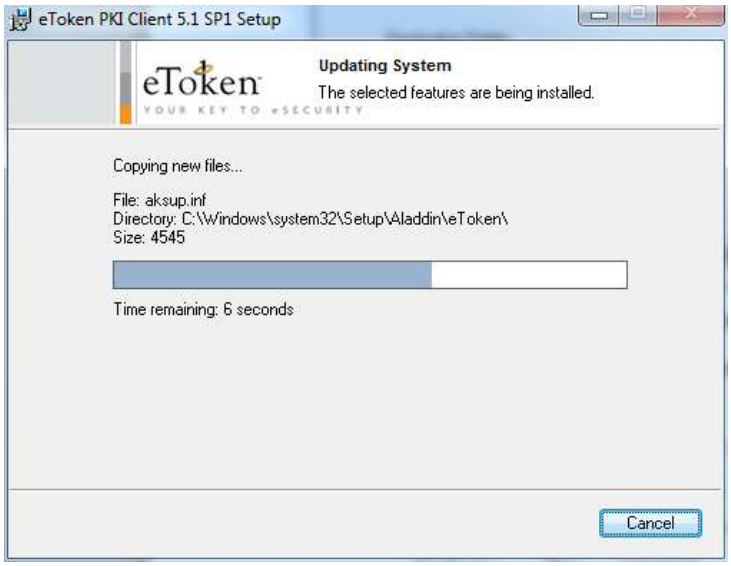


Рисунок 128 – Прогресс установки драйверов eToken

h) После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 129).

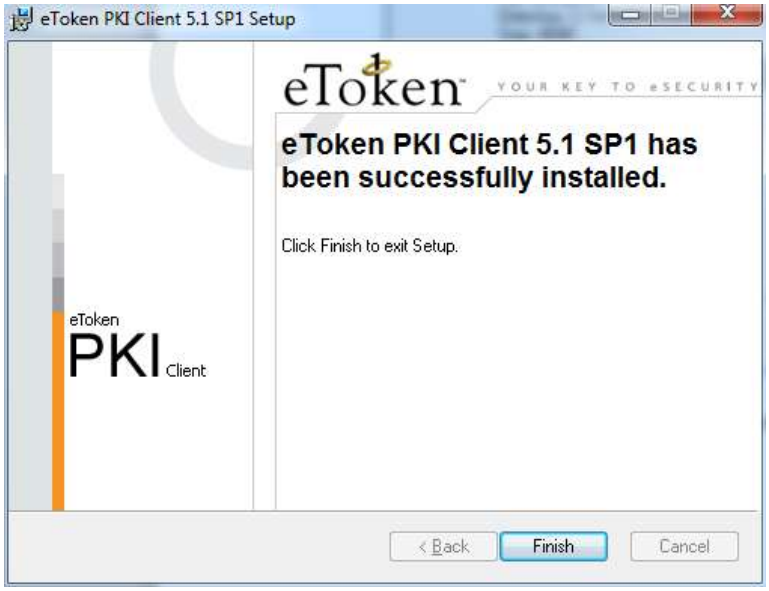


Рисунок 129 – Сообщение об успешной установке драйверов etoken

i) Нажмите кнопку «Finish». Окно установщика драйверов будет закрыто.

j) В случае появления диалога о необходимости перезагрузки АРМ пользователя, перезагрузить АРМ.

3) Для корректного отображения сертификатов на носителе типа eToken дополнительно требуется установка ПК «Единый Клиент JaCarta».

Если ПК «Единый Клиент JaCarta» не установлен, то:

a) Запустите программу-установщик клиента. Окно приветствия установщика единого клиента JaCarta представлено на рисунке (Рисунок 130).

При отсутствии программы-установщика клиента необходимо обратиться к производителю носителя.

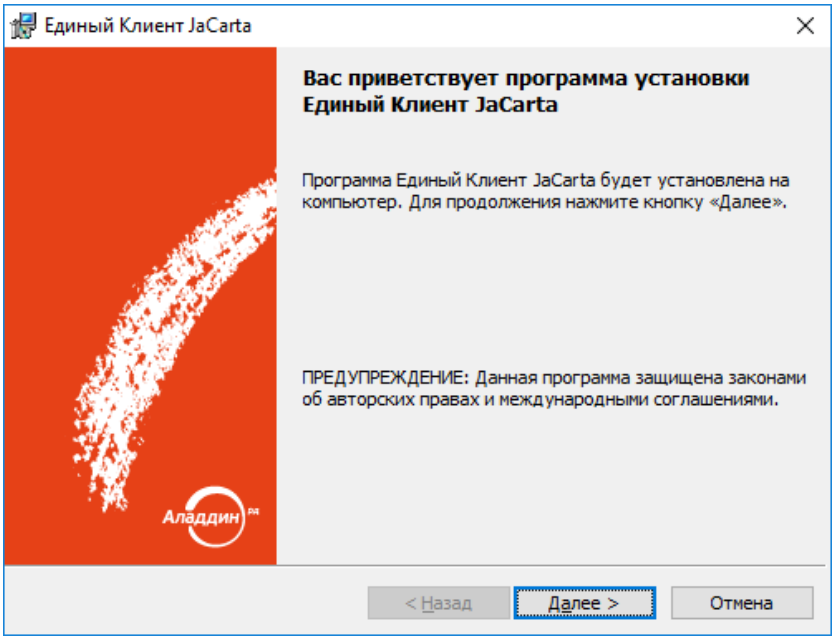


Рисунок 130 – Экранная форма приветствия установщика клиента

b) Нажмите кнопку «Далее». На экране появится диалог «Лицензионное соглашение» (Рисунок 131).

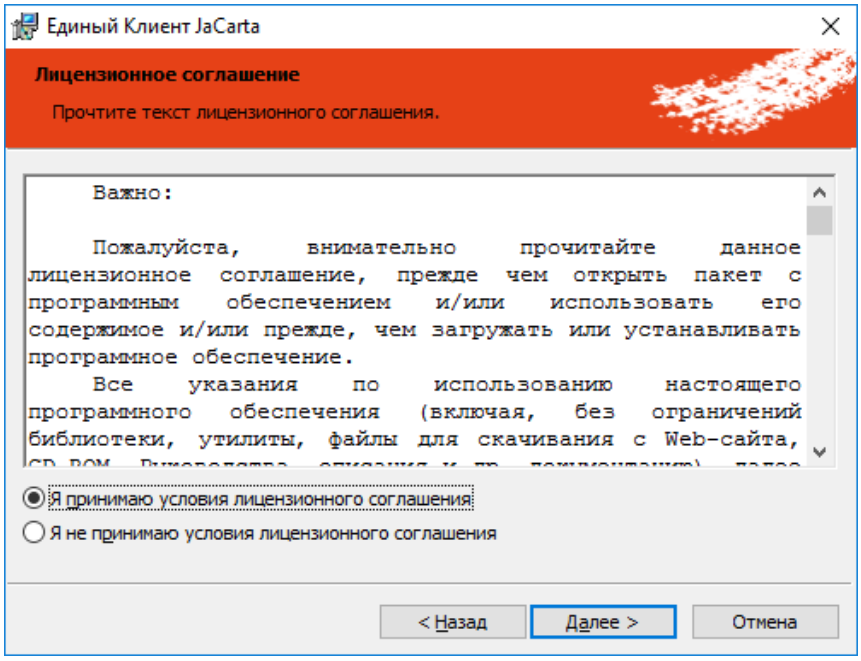


Рисунок 131 – Окно просмотра лицензионного соглашения

c) Выберите пункт «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее». На экране появится диалог выбора вида установки (Рисунок 132).

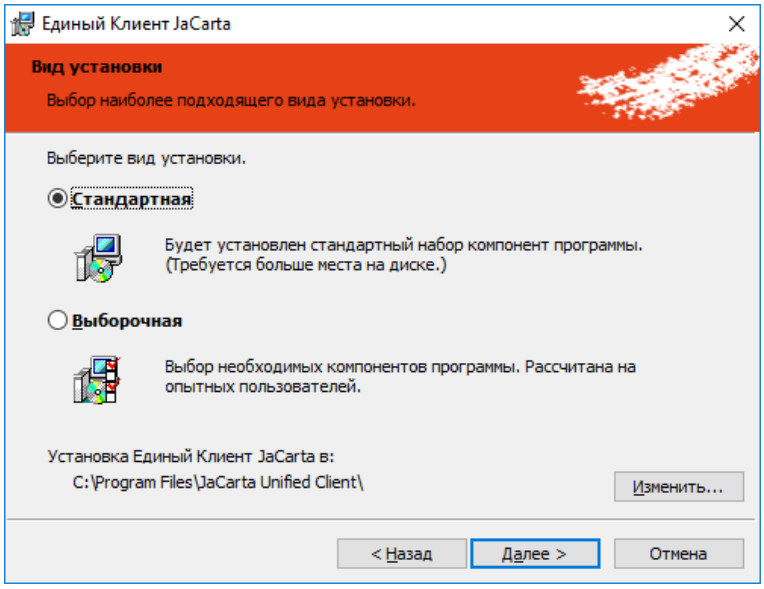


Рисунок 132 – Окно выбора вида установки программы

d) Оставьте вид установки «Стандартная». Нажмите кнопку «Далее». Появится окно установки программы (Рисунок 133). Нажмите кнопку «Установить».

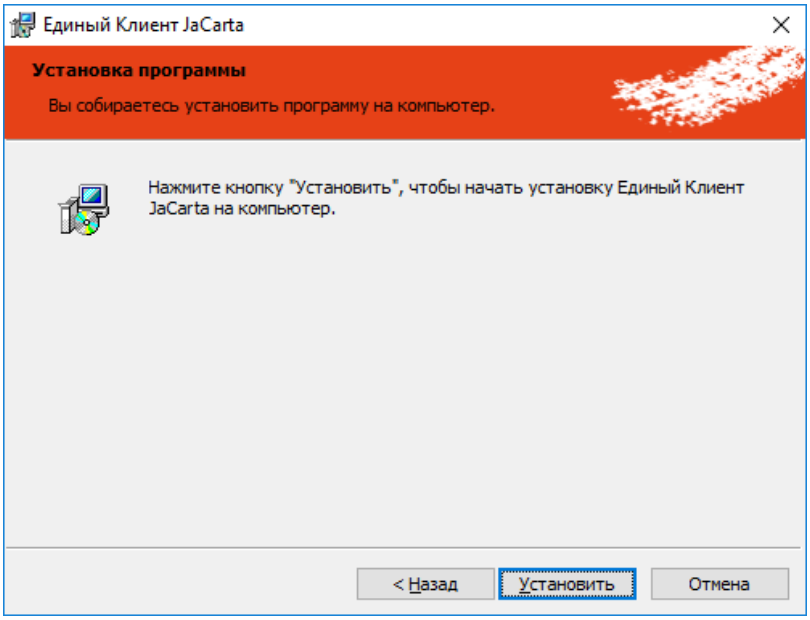


Рисунок 133 – Окно установки программы

e) Начнется установка программы и драйверов. Диалог процесса установки представлен на рисунке (Рисунок 134).

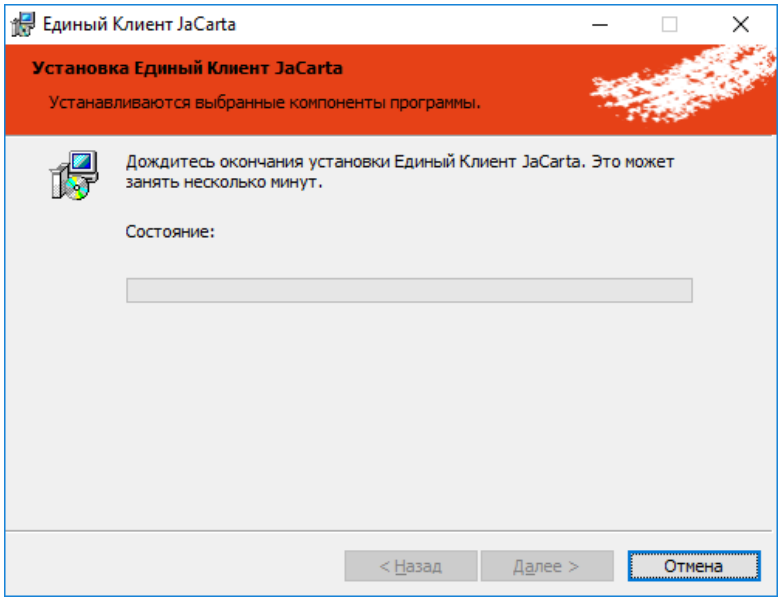


Рисунок 134 – Прогресс установки клиента

f) После завершения установки пользователю будет выведено сообщение об успешной установке клиента, представленное на рисунке (Рисунок 135).

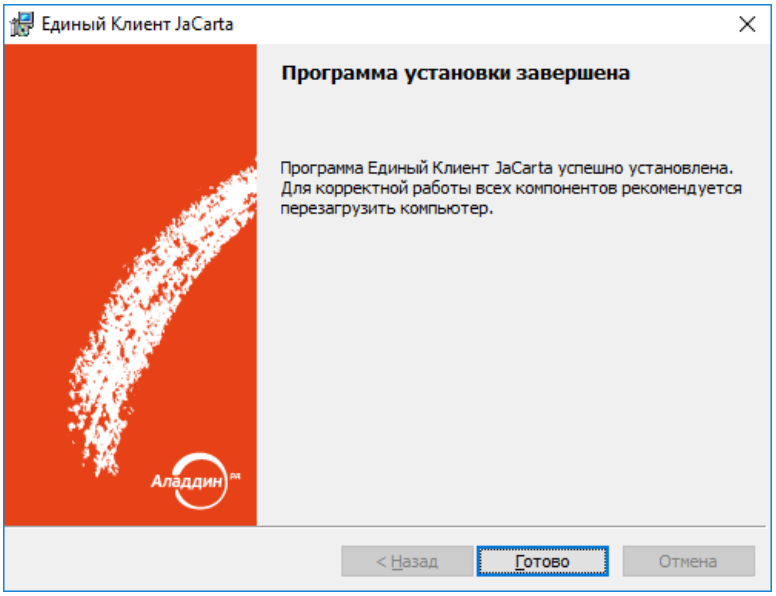


Рисунок 135 – Сообщение об успешной установке драйверов JaCarta

g) Нажмите кнопку «Готово». Окно установщика драйверов будет закрыто.

h) В случае появления диалога о необходимости перезагрузки АРМ пользователя, перезагрузить АРМ.

Б.2.10 Установка СКЗИ «Jinn-Client»

В случае отсутствия дистрибутива необходимо обратиться в территориальный орган Федерального казначейства по месту нахождения. Также можно просмотреть порядок получения дистрибутивов на интернет-сайтах Управлений ФК в разделе ГИС > Удостоверяющий центр.

Рекомендуемая сборка СКЗИ «Jinn-Client» 1.0.3050.0.

Для установки СКЗИ «Jinn-Client» необходимо:

1) В АРМ пользователя вставить носитель информации, содержащий дистрибутив СКЗИ «Jinn-Client».
2) В составе дистрибутива СКЗИ «Jinn-Client» осуществить запуск исполняемого файла «Setup.exe». На экране отобразится меню единого установщика СКЗИ «Jinn-Client» (Рисунок 136).

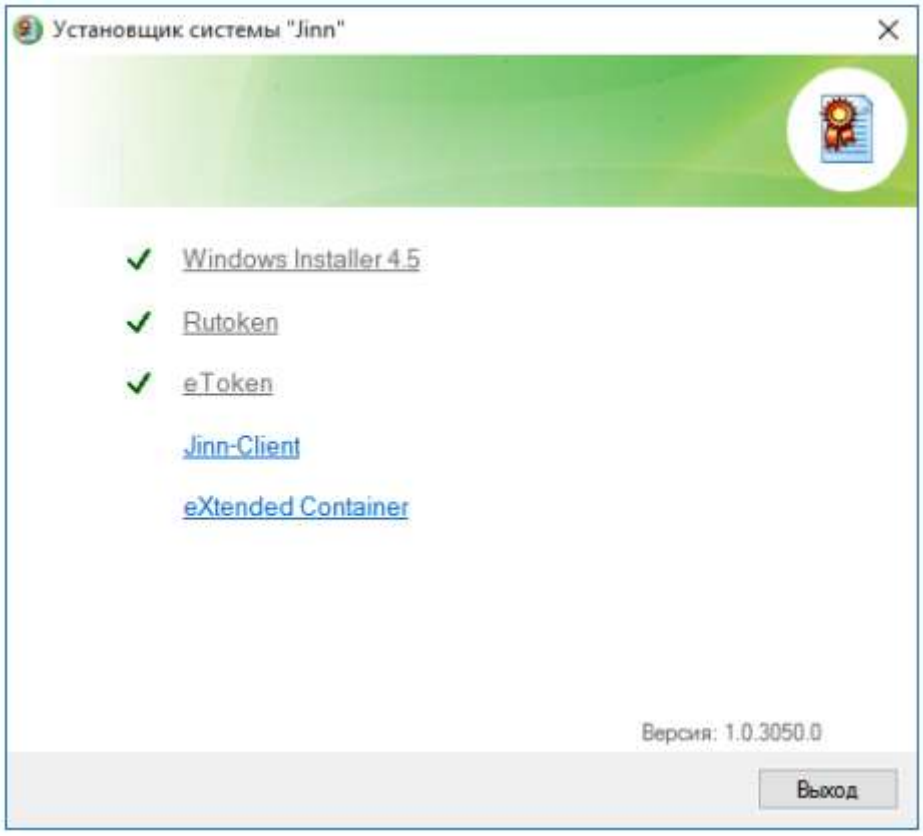


Рисунок 136 – Меню единого установщика СКЗИ «СКЗИ «Jinn-Client»

3) В меню установщика СКЗИ «Jinn-Client» активировать ссылку «Jinn-Client». На экране отобразится диалог приветствия установщика СКЗИ «Jinn-Client» (Рисунок 137).

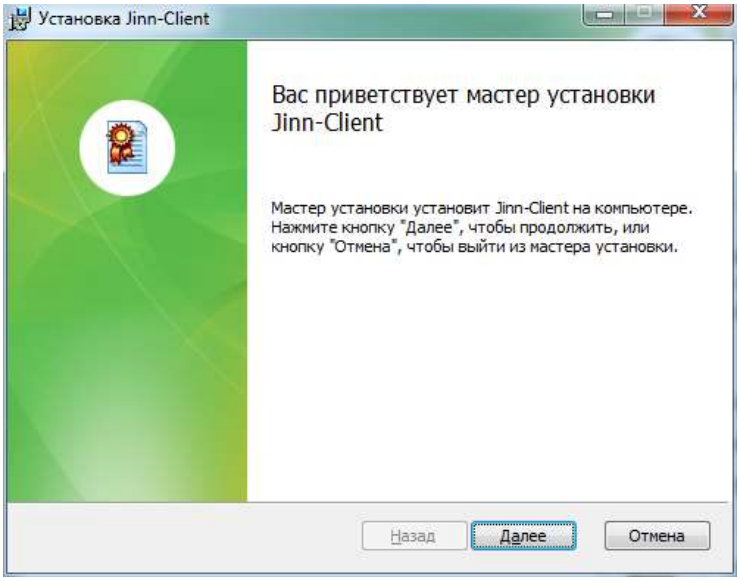


Рисунок 137 – Окно приветствия установщика СКЗИ «Jinn-Client»

4) Для продолжения установки нажмите кнопку «Далее».
5) В появившемся диалоге лицензионного соглашения отметить пункт «Я принимаю условия лицензионного соглашения» (Рисунок 138) и нажать кнопку «Далее».

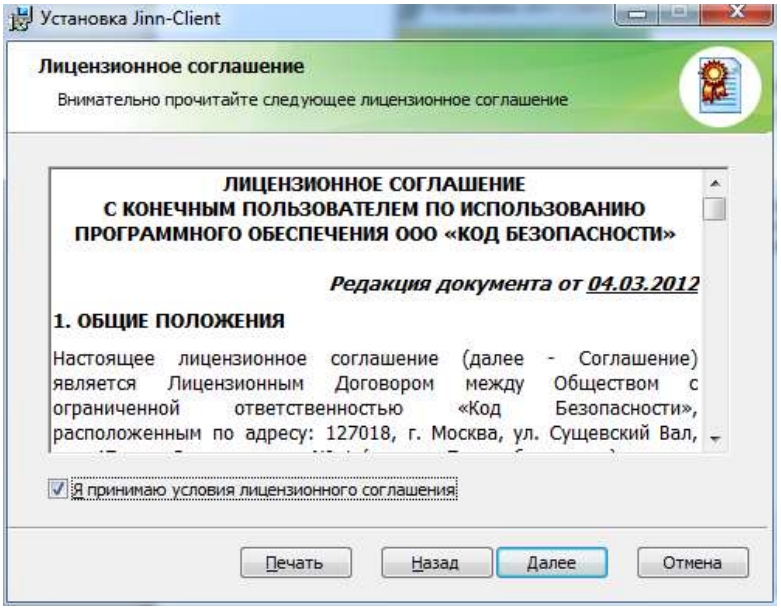


Рисунок 138 – Окно просмотра лицензионного соглашения

6) На экране отобразится диалог ввода лицензионного ключа (Рисунок 139), поставляемого вместе с дистрибутивом СКЗИ «Jinn-Client» в электронном или бумажном виде.

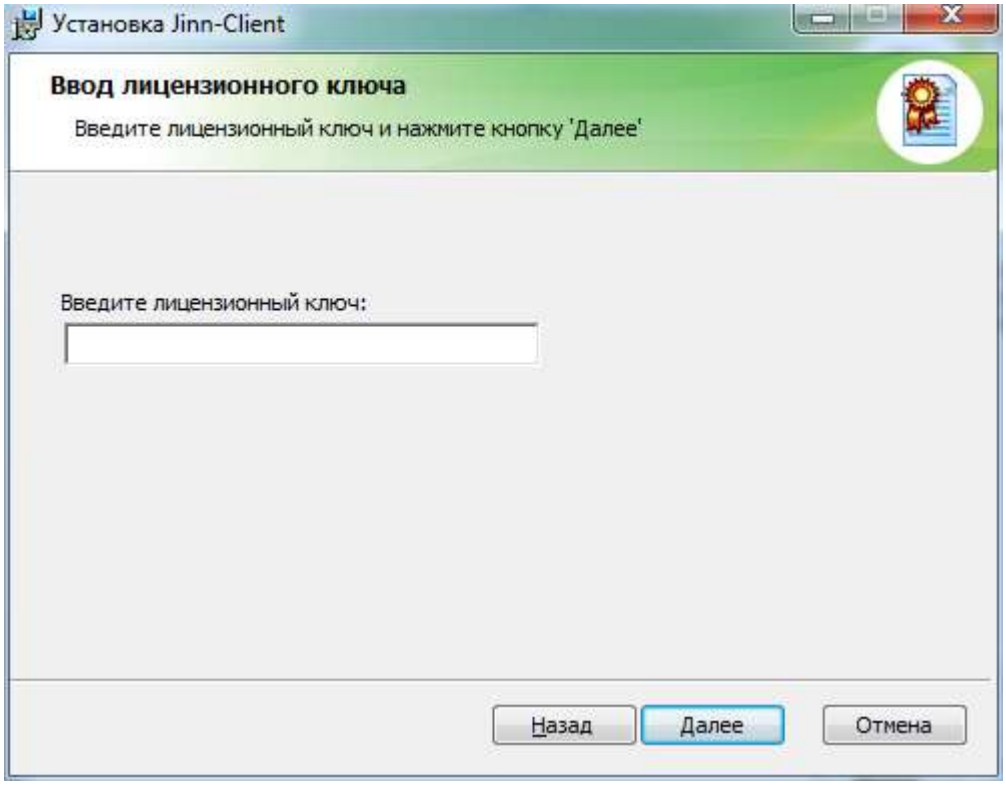


Рисунок 139 – Окно ввода лицензионного ключа

7) Введите лицензионный ключ и нажмите кнопку «Далее». На экране отобразится диалог выбора пути установки СКЗИ «Jinn-Client» (Рисунок 140).

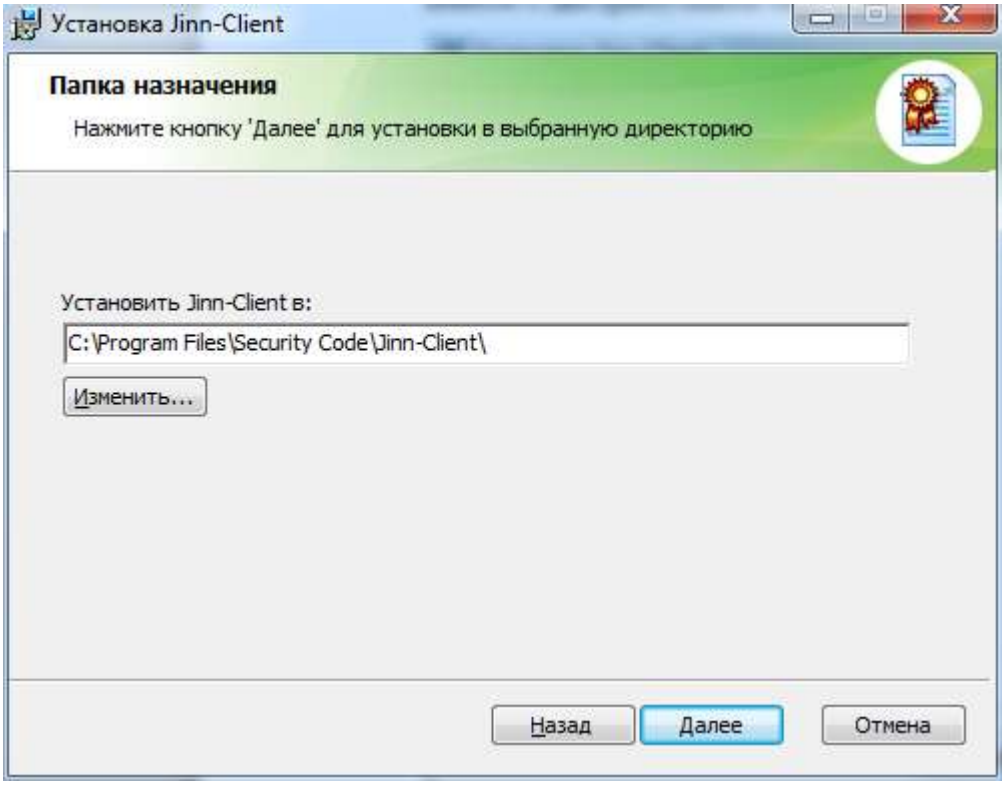


Рисунок 140 – Окно выбора пути установки СКЗИ «СКЗИ «Jinn-Client»

8) Оставьте путь установки по умолчанию. Нажмите кнопку «Далее».
9) В диалоге настройки параметров СКЗИ «Jinn-Client» (Рисунок 141), ничего не изменяя, нажмите кнопку «Далее».

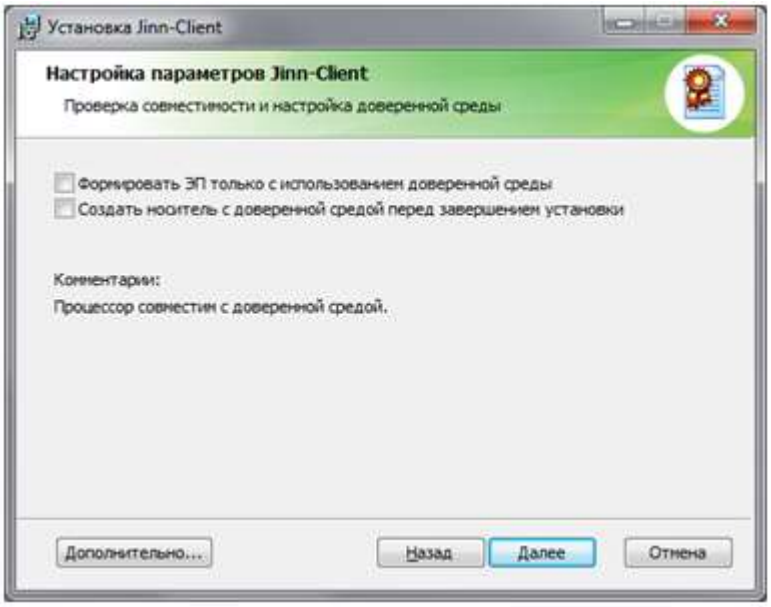


Рисунок 141 – Окно настройки параметров СКЗИ «СКЗИ «Jinn-Client»

Примечание – В случае появления комментария «Процессор не совместим с доверенной средой» выполнять какие-либо действия от пользователя не требуется. Данный комментарий означает, что работа в СКЗИ «Jinn-Client» будет осуществляться без использования режима доверенной среды, процесс установки СКЗИ «Jinn-Client» при этом прерывать не нужно.

10) Далее пользователю будет выведено информационное сообщение о готовности к установке СКЗИ «Jinn-Client» (Рисунок 142).

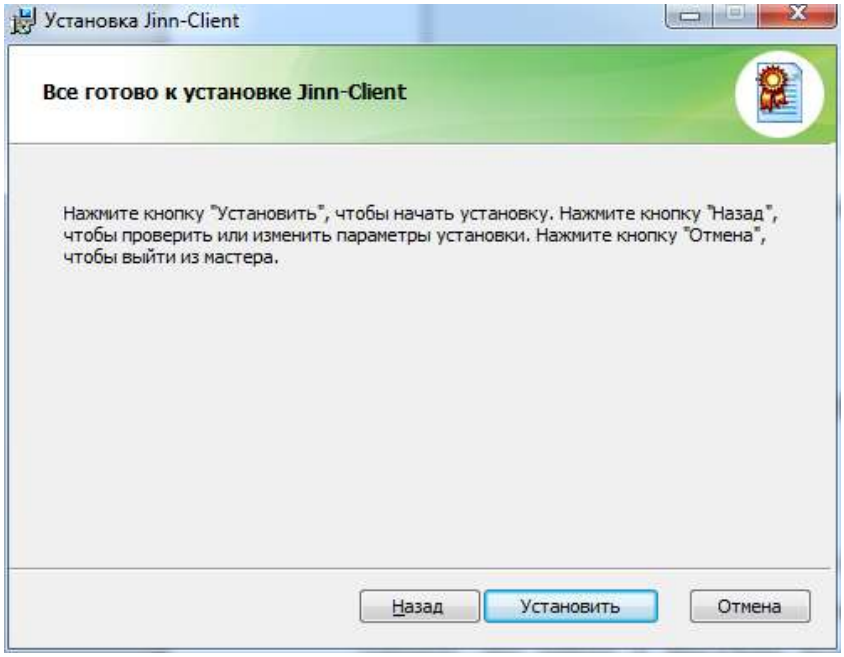


Рисунок 142 – Сообщение о готовности к установке Jinn-Client

11) Нажмите кнопку «Установить». На экране отобразится диалог процесса установки СКЗИ «Jinn-Client» (Рисунок 143).

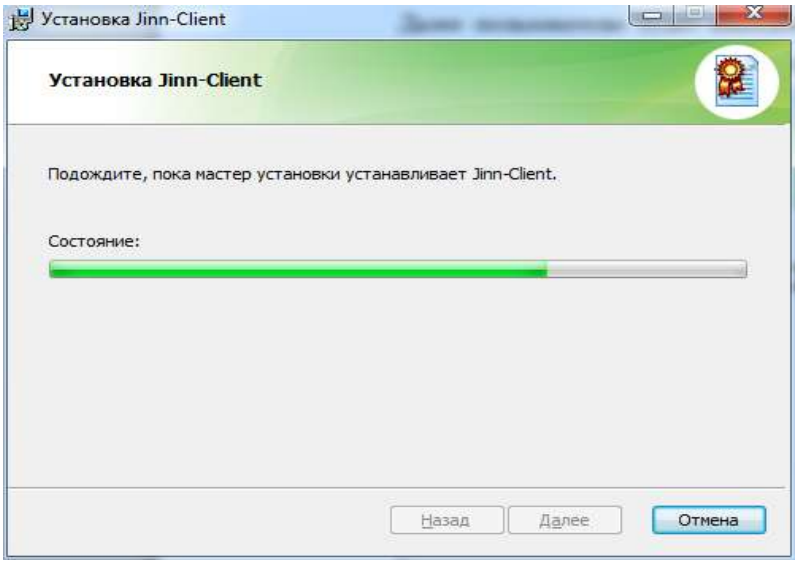


Рисунок 143 – Окно, информирующее пользователя о прогрессе в процессе установки СКЗИ «Jinn-Client»

12)По завершению установки на экран будет выведен диалог об успешном завершении установки (Рисунок 144).

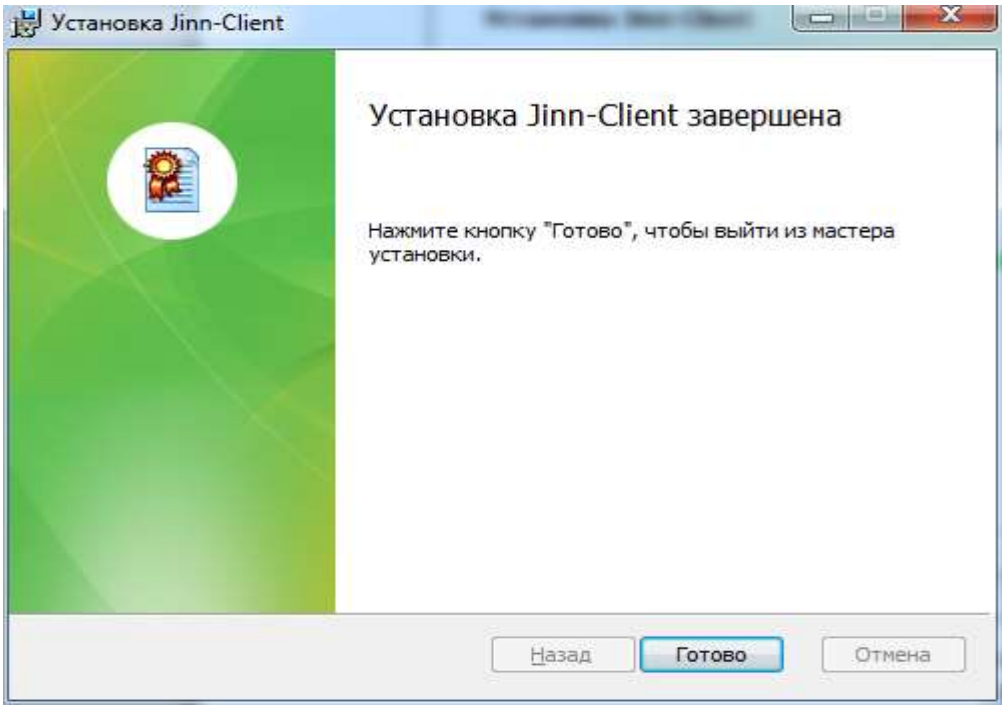


Рисунок 144 – Сообщение об успешном завершении установки СКЗИ «Jinn-Client»

13)Нажмите кнопку «Готово».

Б.2.11 Установка и настройка СКЗИ «Континент TLS VPN Клиент»

В случае отсутствия дистрибутива необходимо обратиться в территориальный орган Федерального казначейства по месту нахождения. Также можно просмотреть порядок получения дистрибутивов на интернет-сайтах Управлений ФК в разделе ГИС > Удостоверяющий центр.

Рекомендуемая для работы с сертификатами на основе ГОСТ 2012 сборка СКЗИ «Континент TLS VPN Клиент» 2.0.1440.0.

Если на АРМ пользователя уже установлен Континент TLS Клиент предыдущей версии, то перед началом установки новой версии требуется выполнить следующие действия:

1) Перейти в Пуск > Панель управления > Программы > Программы и компоненты.
2) Удалить ПО Континент TLS-клиент.
3) Перезапустить АРМ. В процессе удаления появится окно с предложением перезапуска АРМ, необходимо нажать «Да».

Если на АРМ пользователя ранее был установлен криптопровайдер Код Безопасности CSP, который мог устанавливаться отдельно или был встроен в предыдущие версии каких-либо продуктов от производителя «Код Безопасности», то перед началом установки новой версии Континент TLS Клиента требуется удалить остаточные файлы криптопровайдера и очистить реестр специальной утилитой в соответствии со следующей инструкцией:

1) С помощью командной строки запустить утилиту очистки CSP «CspCleaner» с ключами to (Рисунок 145). Запуск должен производиться из директории, в которой находится данная утилита

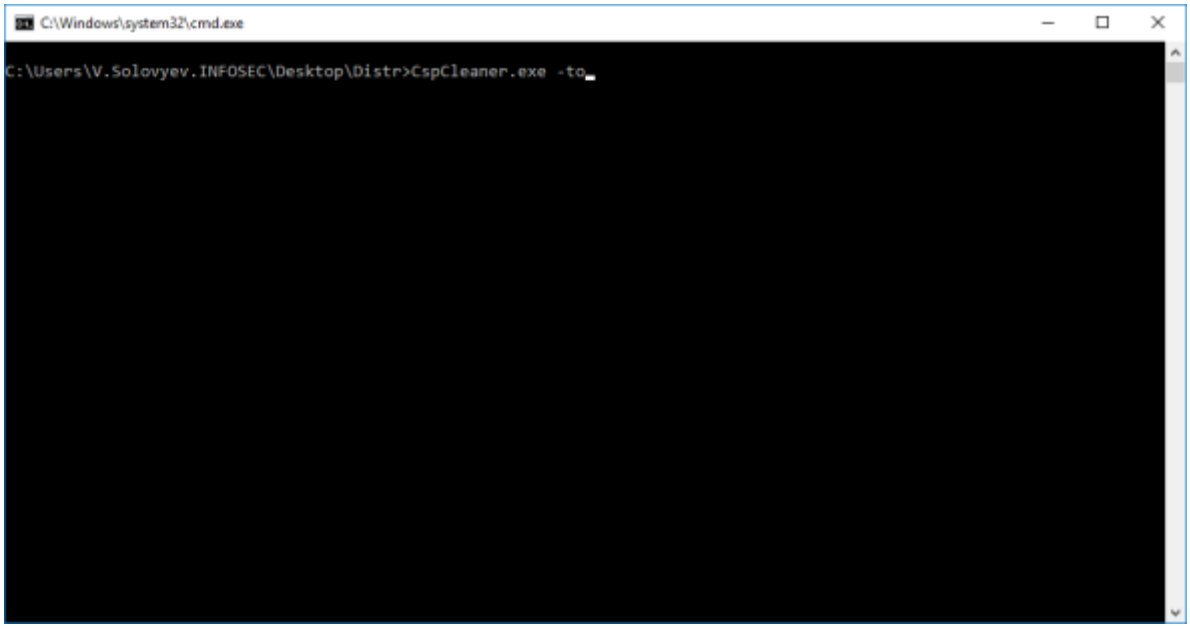


Рисунок 145 – Запуск утилиты очистки CSP

2) После удаления остаточных файлов криптопровайдера согласиться на перезагрузку АРМ.
3) В случае отсутствия дистрибутива утилиты очистки CSP, необходимо скачать дистрибутив с официального сайта производителя.

   Установка и настройка Континент TLS Клиента должна производиться из-под учетной записи с правами администратора на клиентскую операционную систему Windows с установленными обновлениями.

Для установки СКЗИ «Континент TLS VPN Клиент» необходимо:

1) Запустить файл установки «Континент TLS-клиент.exe» (Рисунок 146).

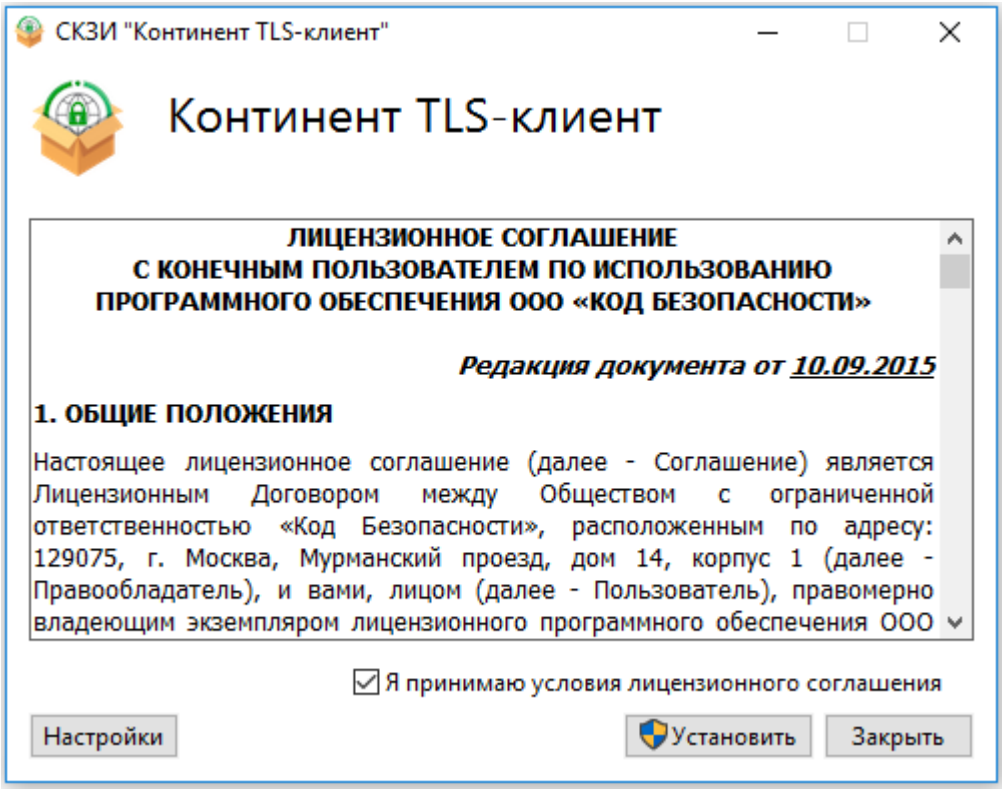


Рисунок 146 – Стартовое окно мастера установки СКЗИ «Континент TLS VPN Клиент»

2) Отметить чекбокс «Я принимаю условия лицензионного соглашения». Нажать кнопку «Установить».
3) Начнется процесс установки.
4) При успешной установке отобразится диалоговое окно «Установка завершена» (Рисунок 147).

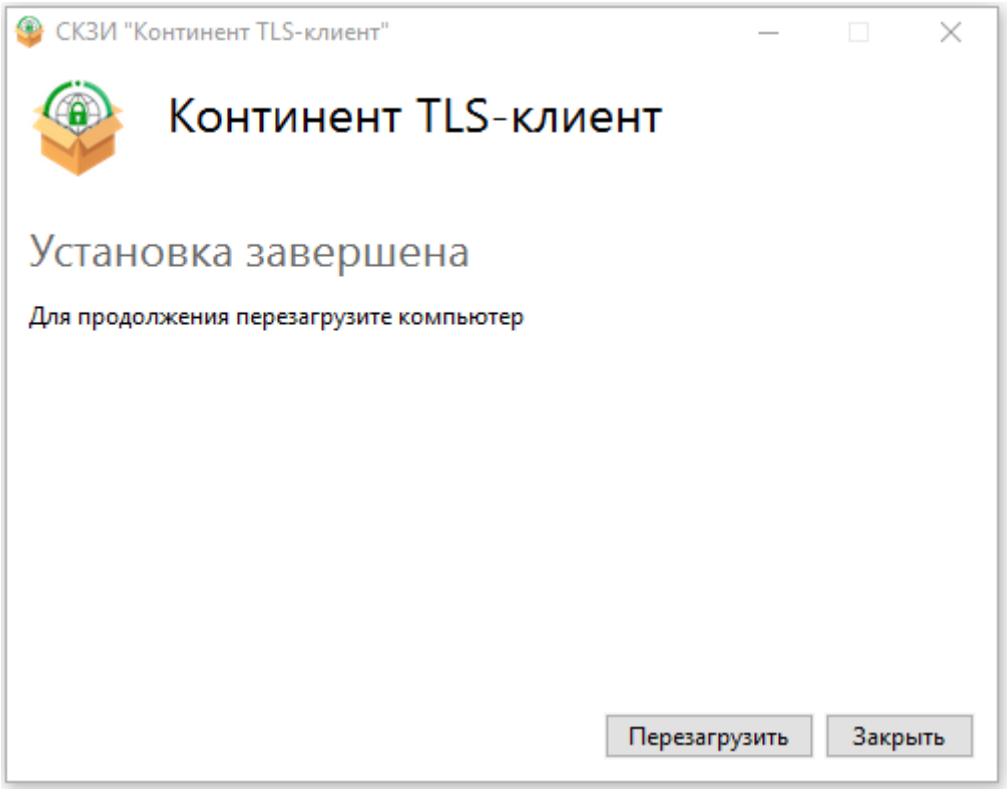


Рисунок 147 – Диалоговое окно завершения установки

5) Нажмите кнопку «Перезагрузить». АРМ перезагрузится.

В случае если на АРМ установлено какое-либо антивирусное ПО, оно может блокировать работу Континент TLS Клиента, поэтому после установки данного СКЗИ необходимо добавить Континент TLS Клиент в доверенное программное обеспечение антивируса и перезагрузить АРМ.

При первичной установке СКЗИ «Континент TLS VPN Клиент» на АРМ требуется выполнить регистрацию СКЗИ.

Во время первого запуска СКЗИ «Континент TLS VPN Клиент» отобразится диалоговое окно «Вы используете незарегистрированную версию программы» (Рисунок 148). При нажатии на кнопку «Продолжить без регистрации» пользователю будет предоставлен демонстрационный период эксплуатации СКЗИ продолжительностью 14 дней. По истечении данного срока, работа в TLS Клиенте будет невозможна.

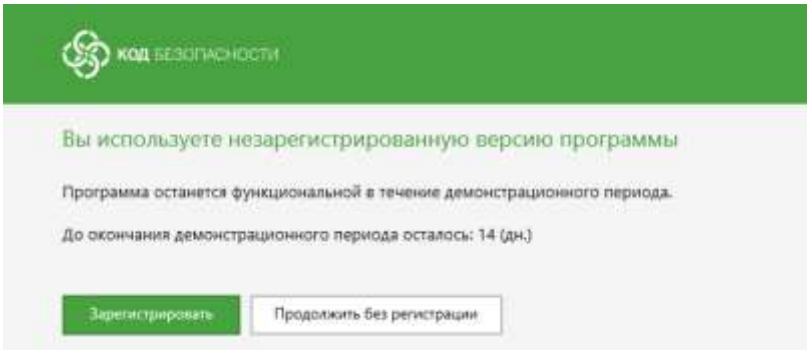


Рисунок 148 – Диалоговое окно о состоянии регистрации СКЗИ

В зависимости от способа доступа к подсистеме (из сети ЗКВС или из сети Интернет) требуется выбрать тип регистрации.

В случае если доступ к подсистеме производится из сети Интернет, необходимо:

6) В появившемся диалоговом окне нажать на кнопку «Зарегистрировать». Отобразится окно регистрации. Перейти в окно регистрации можно также из меню TLS Клиента, нажав на вкладку «Настройки». Перейти в раздел «Регистрация». Нажать на кнопку «Начать» под полем «Онлайн-регистрация» (Рисунок 149).



Рисунок 149 – Вкладка «Настройки», раздел «Регистрация». Континент TLS Клиент

7) Заполнить все необходимые поля (Рисунок 150). Если адрес сервера регистрации не указан изначально, указать: «registration.securitycode.ru». Выбрать необходимый класс защиты.

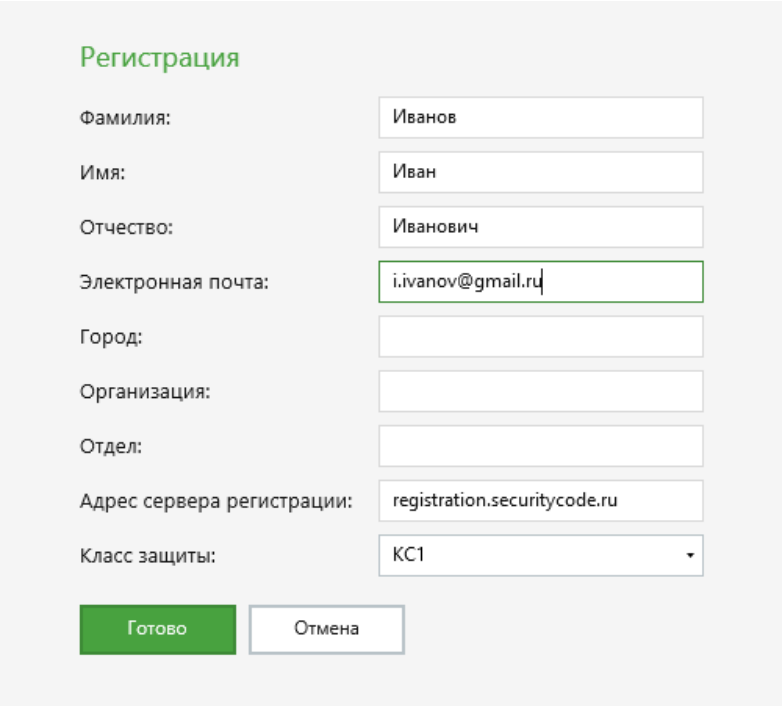


Рисунок 150 – Окно регистрации СКЗИ

8) Нажать кнопку «Готово».

Для настройки СКЗИ «Континент TLS VPN Клиент» необходимо:

1) Запустить СКЗИ «Континент TLS VPN Клиент» (Рисунок 151), нажав на соответствующий ярлык на рабочем столе.

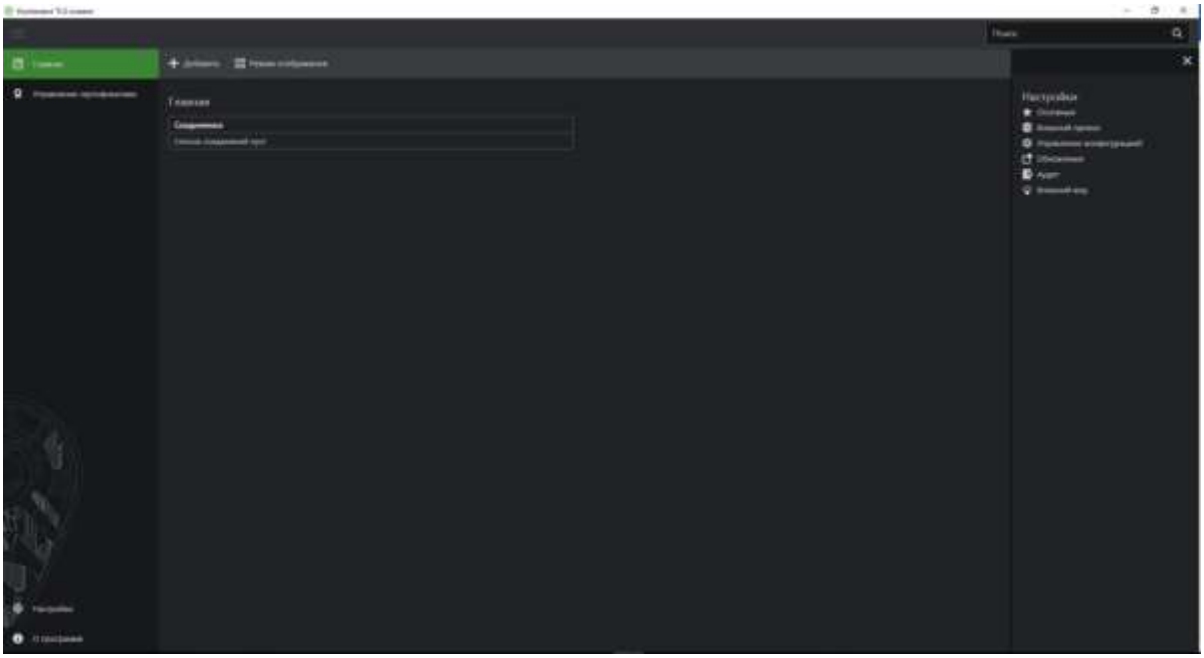


Рисунок 151 – Вкладка «Главная». Континент TLS Клиент

2) Откроется меню соединений – вкладка «Главная»
3) Нажать на кнопку «Добавить». Выбрать тип соединения «Ресурс» В окне добавления ресурса прописать следующие параметры.
    a) Точка входа в подсистему по сертификатам пользователей на основе ГОСТ Р 34.10-2012:
        — Адрес: <мнемоника ИС ФК>.cert.roskazna.ru/<адрес сервиса управления доступом>.
        — Имя ресурса: <мнемоника ИС ФК>.cert.roskazna.ru/<адрес сервиса управления доступом>.
        — Удаленный порт: 443
        — Тип: Прокси
    b) Точка входа в подсистему посредством сервиса ЕСИА:
        — Адрес: <мнемоника ИС ФК>.esia.roskazna.ru/<адрес сервиса управления доступом>.
        — Имя ресурса: <мнемоника ИС ФК>.esia.roskazna.ru/<адрес сервиса управления доступом>.
        — Удаленный порт: 443
        — Тип: Прокси

c) Точка входа в подсистему посредством ввода логина (СНИЛС или ИНН) и пароля:

— Адрес: <мнемоника ИС ФК>.login.roskazna.ru/<адрес сервиса управления доступом>.

— Имя ресурса: <мнемоника ИС ФК>.login.roskazna.ru/<адрес сервиса управления доступом>.

— Удаленный порт: 443

— Тип: Прокси

4) После введения параметров нажать кнопку «Сохранить». Окно соединений будет выглядеть следующим образом (Рисунок 152):

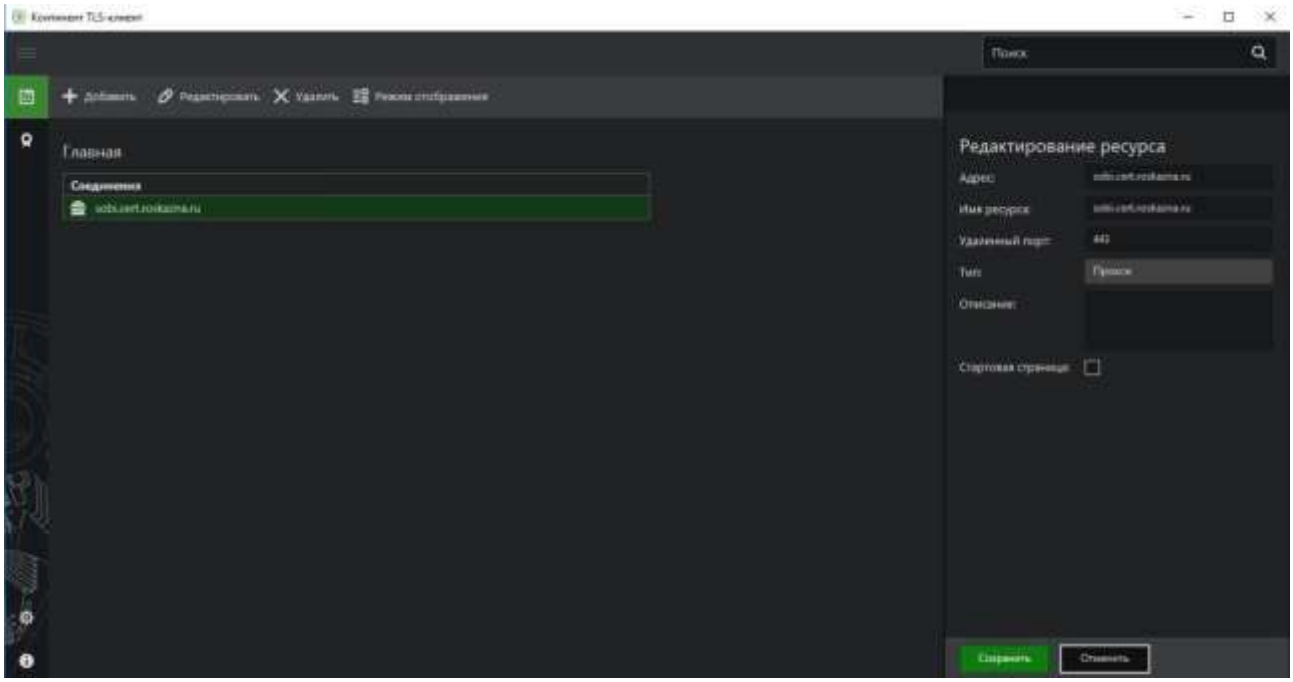


Рисунок 152 – Вкладка «Главная». Настройка соединений. Континент TLS Клиент

5) Перейти на вкладку «Настройки». Выбрать раздел «Основные».
6) Необходимо отметить следующие чекбоксы:
   a) Проверять сертификаты по CRL.
   b) Скачивать CRL автоматически.
   c) Запускать при старте системы.
   d) При запуске свернуть в системный трей.
7) Нажать кнопку «Сохранить».

Окно основных настроек должно выглядеть следующим образом (Рисунок 153):

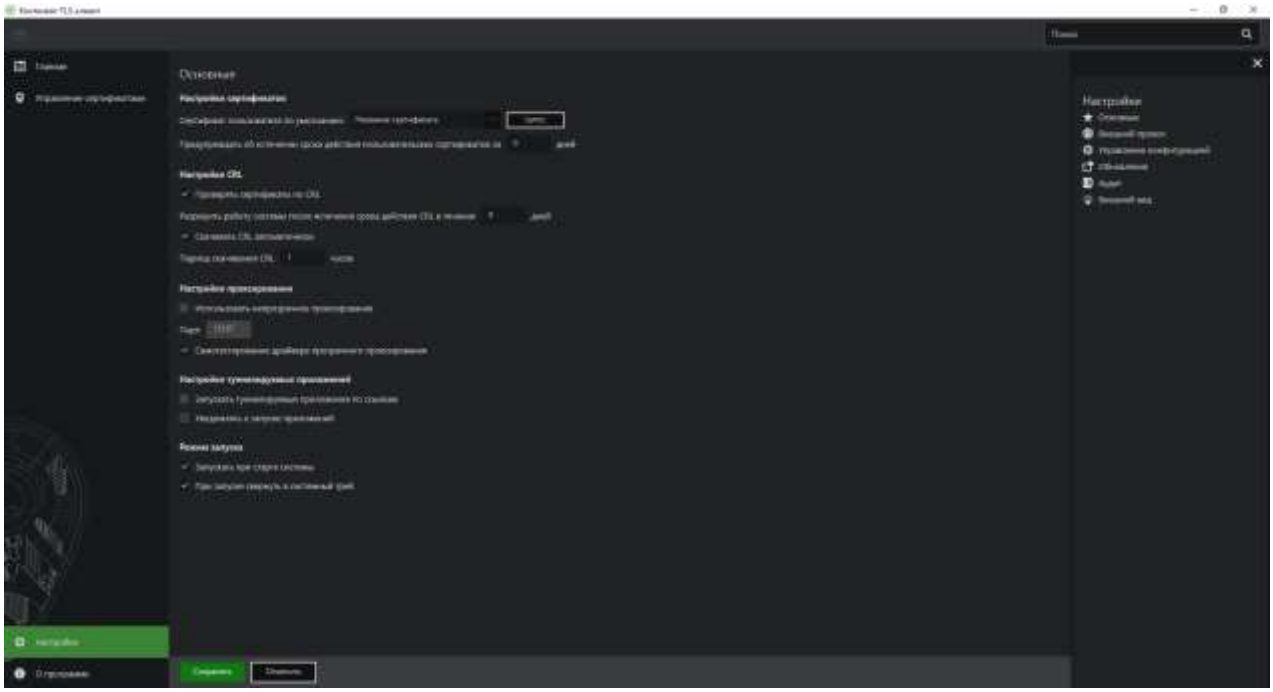


Рисунок 153 – Вкладка «Настройки». Раздел «Основные». Континент TLS Клиент

8) Перейти в раздел «Внешний прокси».
9) Отметить чекбокс «Настраивать автоматически».
   a) В случае если в организации используется прокси-сервер, после сохранения настроек его параметры определятся автоматически.
   b) Если прокси-сервер не используется, после сохранения окно параметров останется пустым.

Окно настроек внешнего прокси должно выглядеть следующим образом (Рисунок 154):

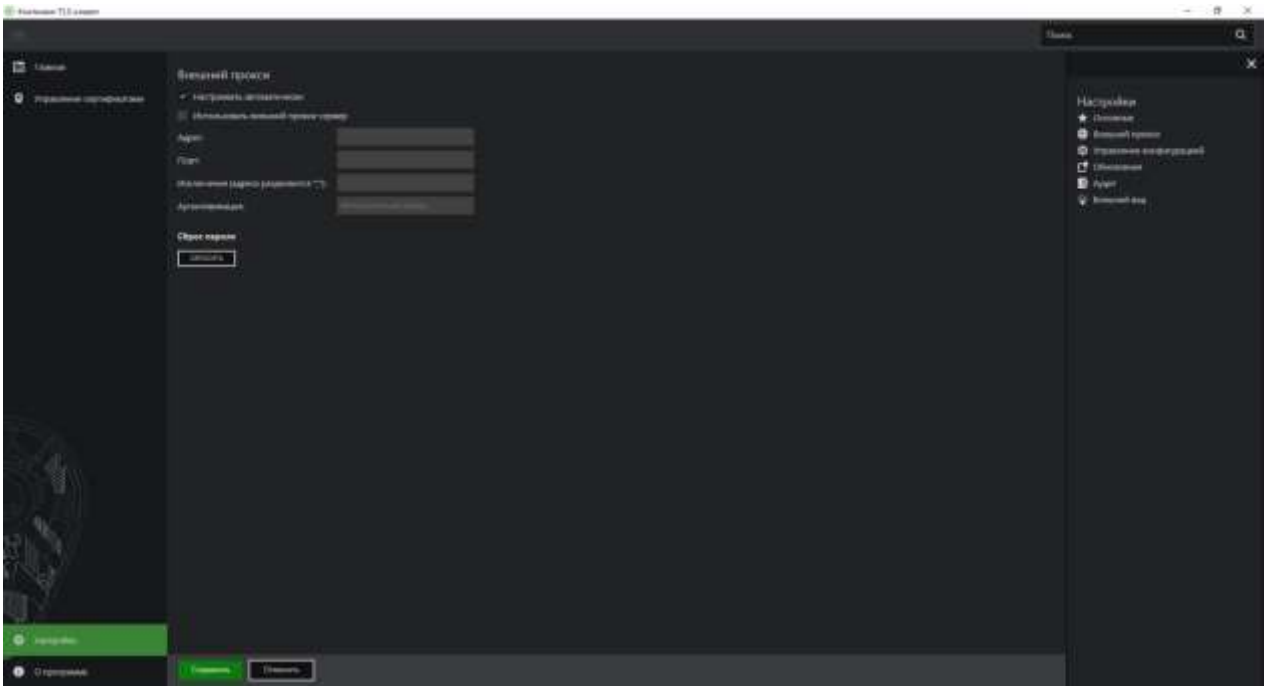


Рисунок 154 – Вкладка «Настройки». Раздел «Внешний прокси». Континент TLS Клиент

10)Перейти на вкладку «Управление сертификатами» (Рисунок 155). Выбрать раздел «Серверные сертификаты».

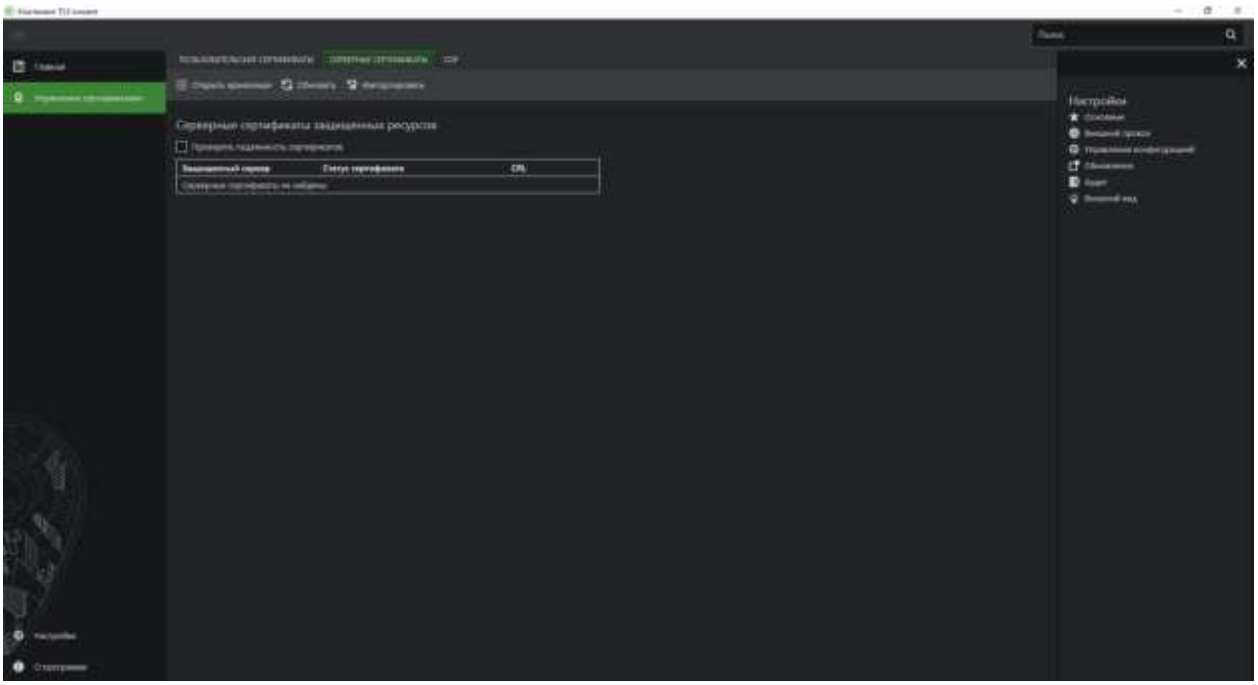


Рисунок 155 – Вкладка «Управление сертификатами»

11)Нажать на кнопку «Импортировать». В открывшемся меню выбрать необходимый сертификат сервера в зависимости от используемой точки входа (Рисунок 156).

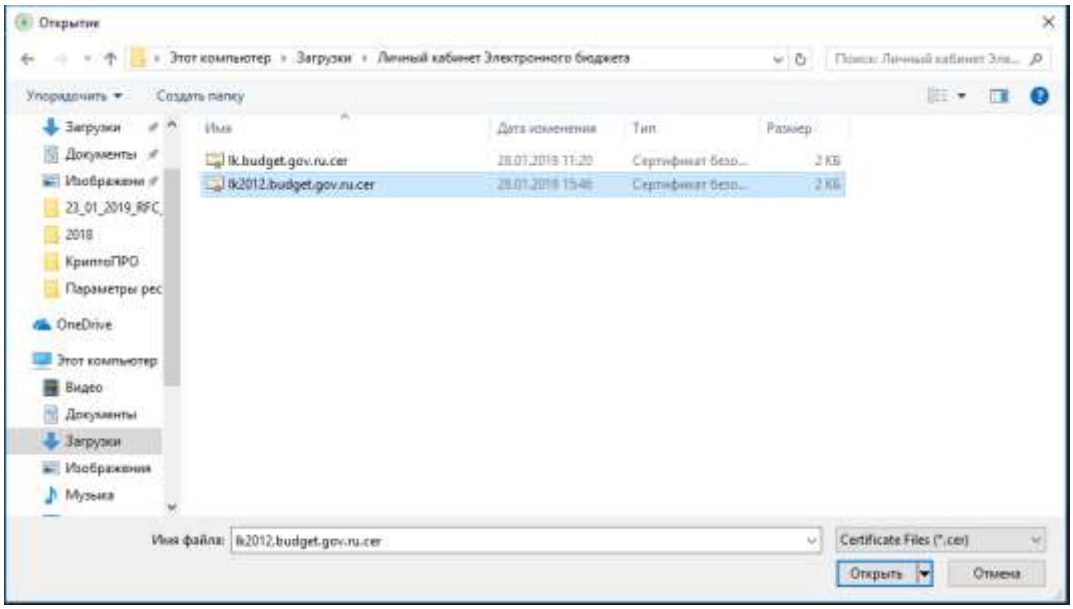


Рисунок 156 – Выбор серверного сертификата

12)Пример окна серверных сертификатов представлен на рисунке 157.

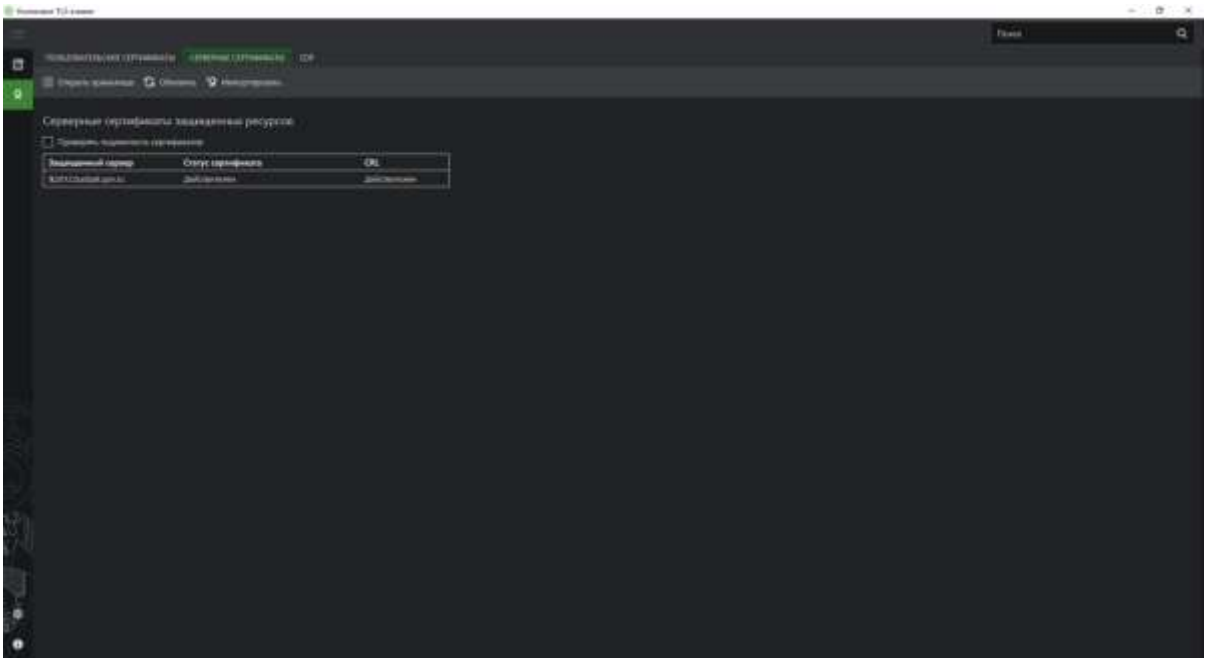


Рисунок 157 – Пример заполненного окна серверных сертификатов

13)Перейти в раздел «Пользовательские сертификаты» (Рисунок 158).

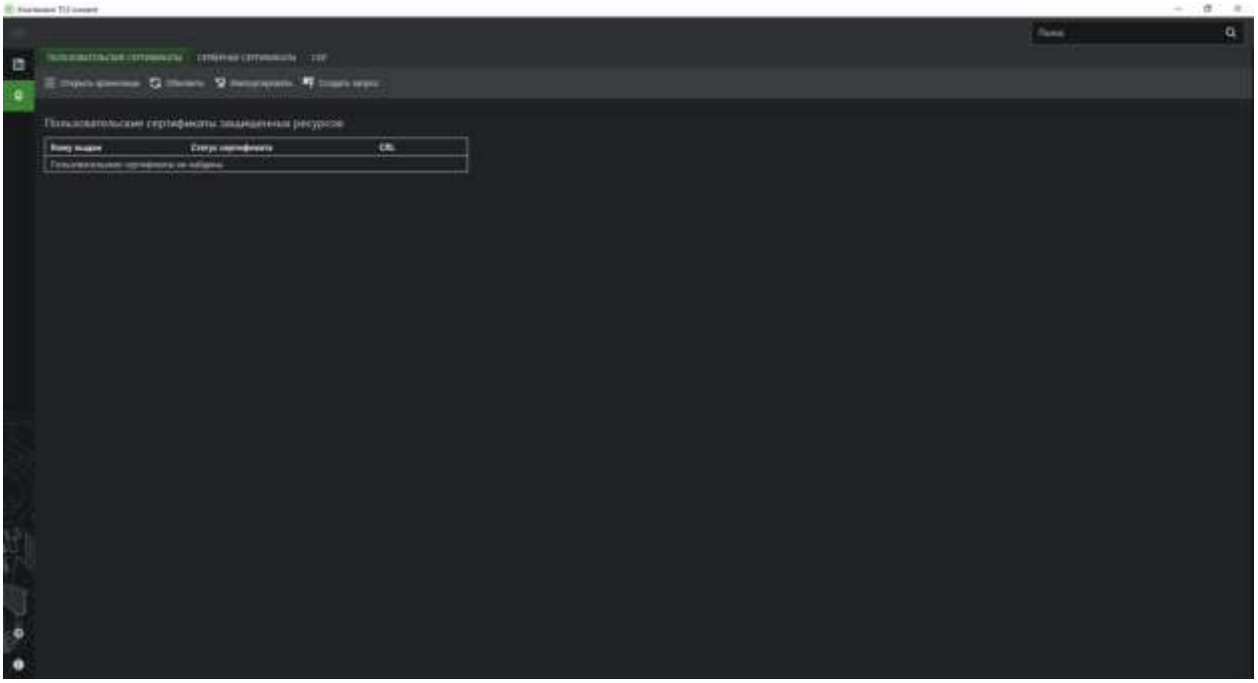


Рисунок 158 – Вкладка «Управление сертификатами»

14) В случае если в окне пользовательских сертификатов отсутствуют требуемые сертификаты, необходимо произвести установку сертификата в криптоконтейнер на носителе с помощью криптопровайдера КриптоПро CSP. Для этого нужно выполнить следующие действия:

   a) Открыть КриптоПро CSP и перейти на вкладку «Сервис» (Рисунок 159).

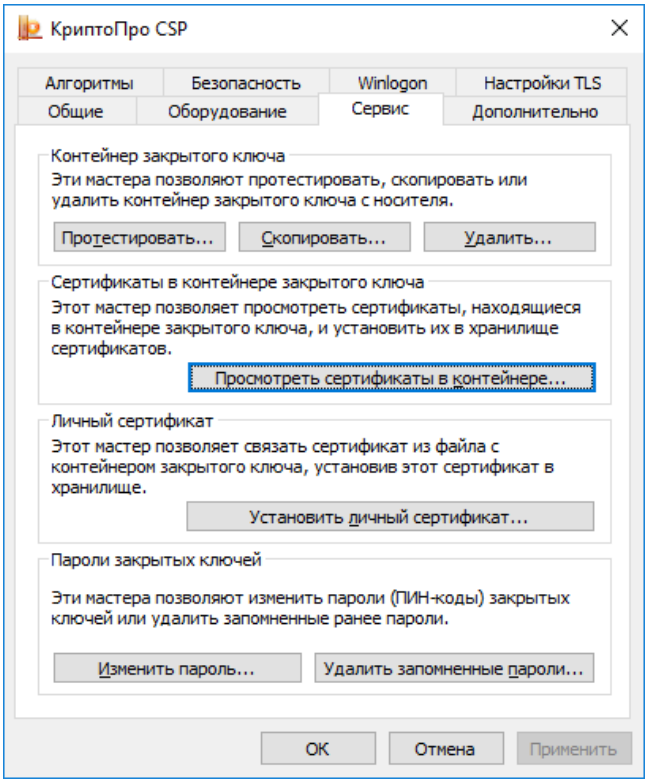


Рисунок 159 – Вкладка «Сервис». КриптоПро CSP

b) Нажать на кнопку «Установить личный сертификат».

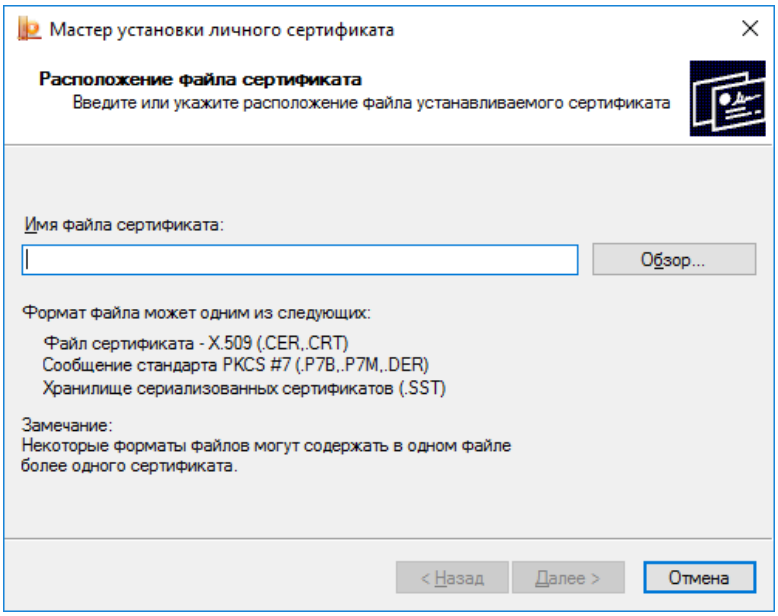


Рисунок 160 – Расположение файла сертификата. КриптоПро CSP

c) В появившемся меню нажать на кнопку «Обзор…» (Рисунок 160).

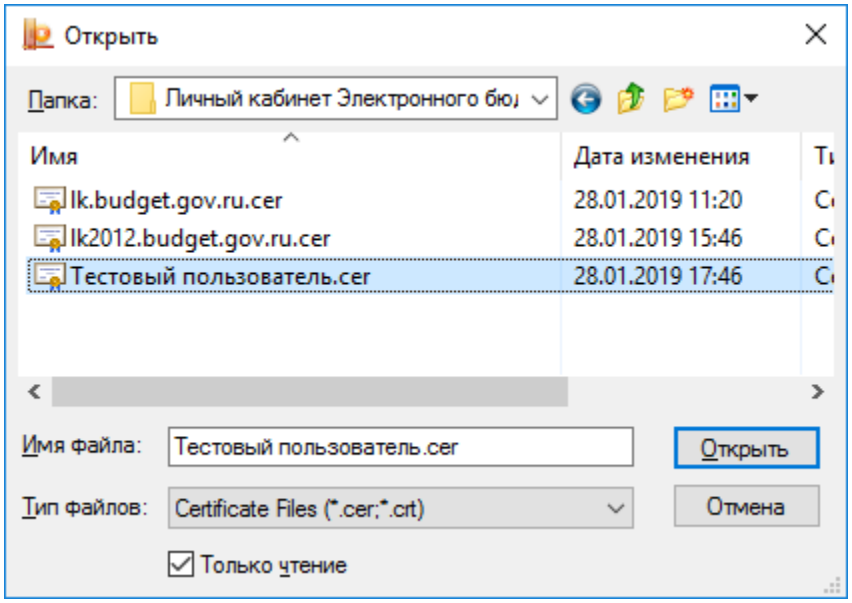


Рисунок 161 – Выбор сертификата. КриптоПро CSP

d) Выбрать необходимый сертификат. Нажать кнопку «Открыть» (Рисунок 161).

e) Дважды нажать кнопку «Далее».

Откроется окно выбора контейнера закрытого ключа (Рисунок 162).

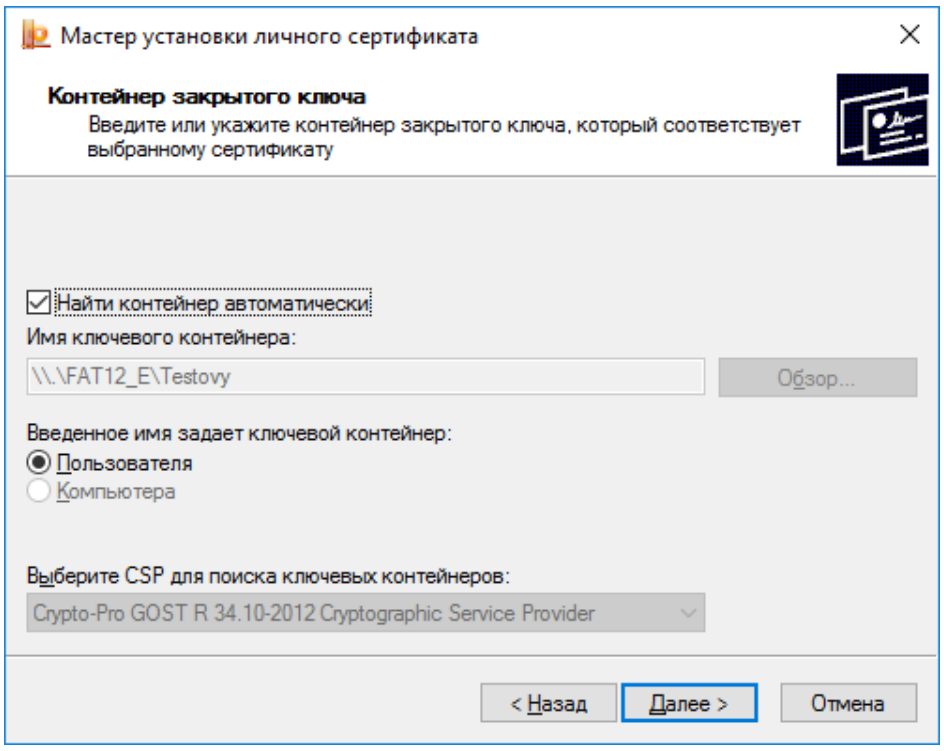


Рисунок 162 – Выбор контейнера закрытого ключа. КриптоПро CSP

f) Отметить чекбокс «Найти контейнер автоматически». Контейнер должен находится на съемном носителе. Нажать кнопку «Далее».

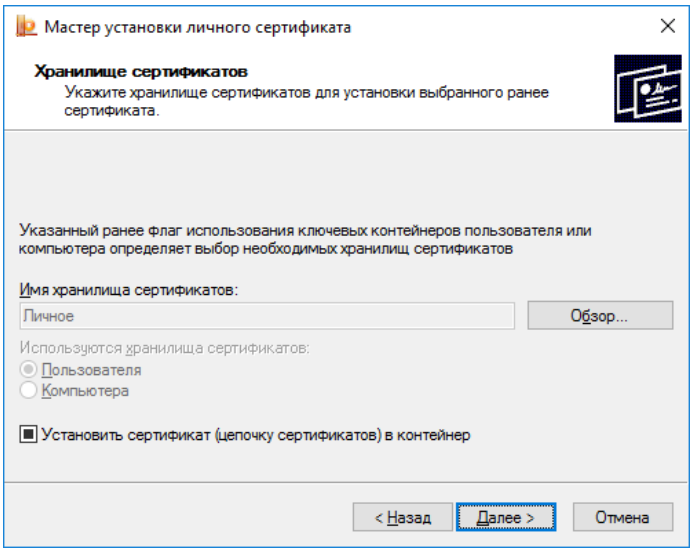


Рисунок 163 – Хранилище сертификатов. КриптоПро CSP

g) Отметить чекбокс «Установить сертификат в контейнер» (Рисунок 163). Нажать кнопку «Далее».

h) Отобразится окно завершения установки сертификата в контейнер (Рисунок 164).

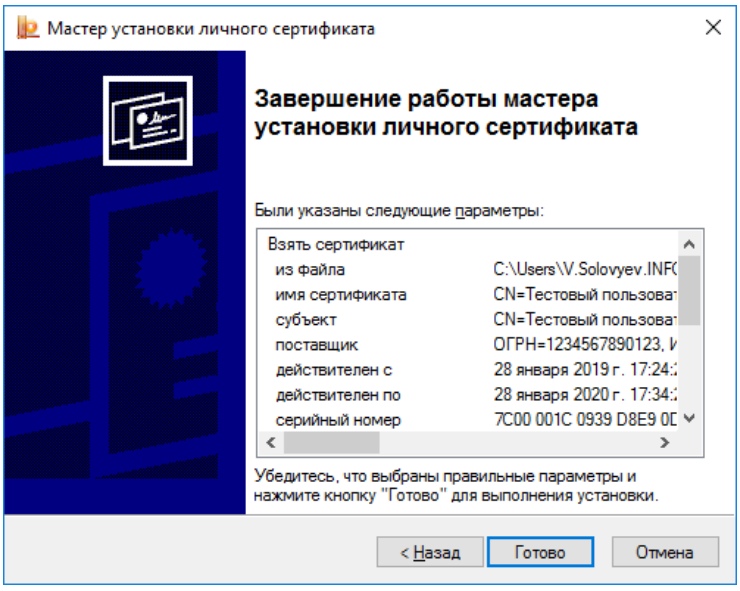


Рисунок 164 – Завершение установки сертификата в контейнер. КриптоПро CSP

i) Нажать кнопку «Готово».

15) Обновить окно пользовательских сертификатов в Континент TLS Клиенте (Рисунок 165).

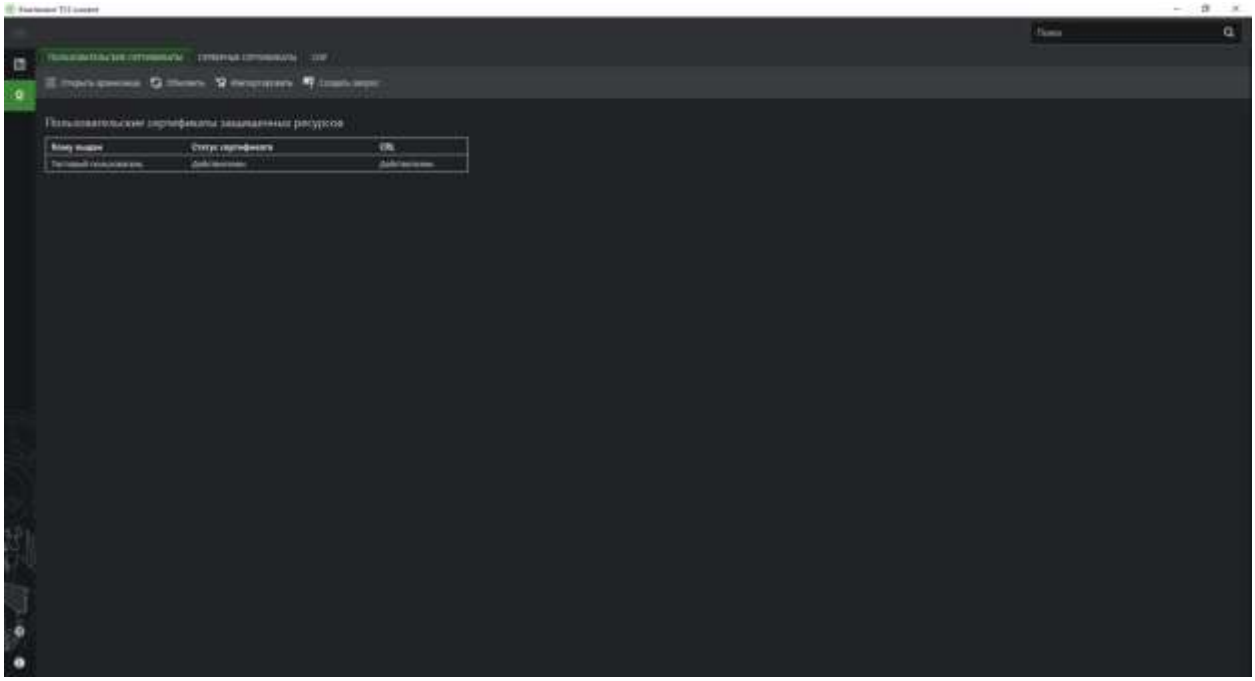


Рисунок 165 – Окно пользовательских сертификатов. Континент TLS Клиент

16)Перейти в раздел CDP и нажать кнопку «Скачать CRL» (Рисунок 166).

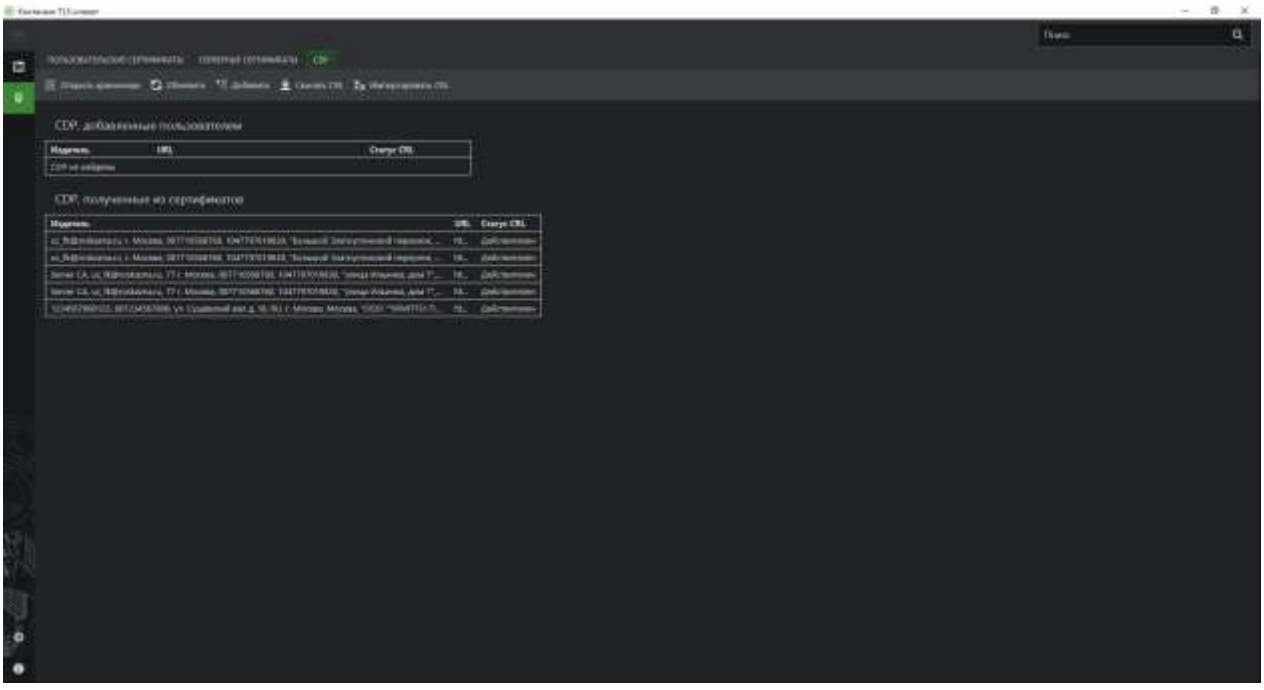


Рисунок 166 – Окно CDP. Континент TLS Клиент

17)В правом нижнем окне рабочего стола нажать на значок «Континент TLS Клиента» правой кнопкой мыши и выбрать пункт «Сброс соединений».

Б.2.12 Установка опционального ПО "eXtended Container"

Опциональное ПО "eXtended Container" (XC) требуется для корректного отображения в Jinn-Client сертификатов на носителях, выданных на основе ГОСТ 2012.

Установка XC должна производиться строго из дистрибутива Jinn-Client после установки TLS Клиента **с предварительным удалением ПО "eXtended Container"(XC) версии 1.0.2.2**.

Рекомендуемая для работы с сертификатами на основе ГОСТ 2012 сборка Версия XC 1.0.1.1.

Для установки опционального ПО "eXtended Container" необходимо:

1) В АРМ пользователя вставить носитель информации, содержащий дистрибутив СКЗИ «Jinn-Client».
2) В составе дистрибутива СКЗИ «Jinn-Client» осуществить запуск файла «xc.msi» для 32-разрядной ОС или «xc64.msi» для 64-разрядной ОС, находящиеся в папке «Jinn» дистрибутива. На экране отобразится меню мастера установки опционального ПО "eXtended Container" (Рисунок 167).

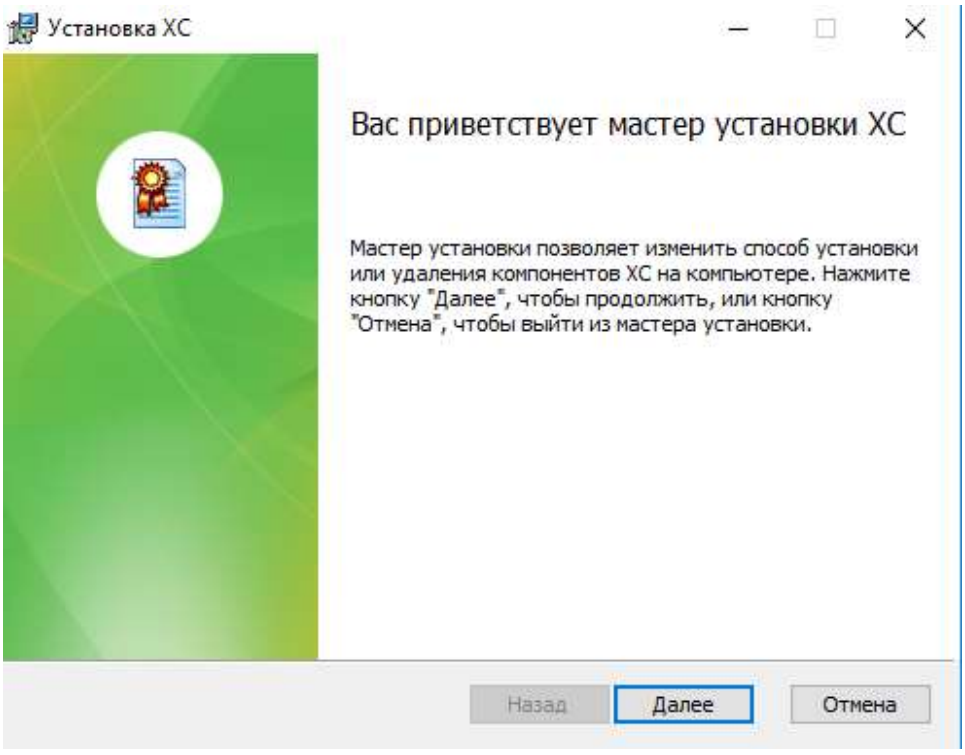


Рисунок 167 – Окно приветствия установщика опционального ПО "eXtended Container"

3) Для продолжения установки нажмите кнопку «Далее».

На экране отобразится диалог ввода лицензионного ключа (Рисунок 168), поставляемого вместе с дистрибутивом СКЗИ «Jinn-Client» в электронном или бумажном виде.

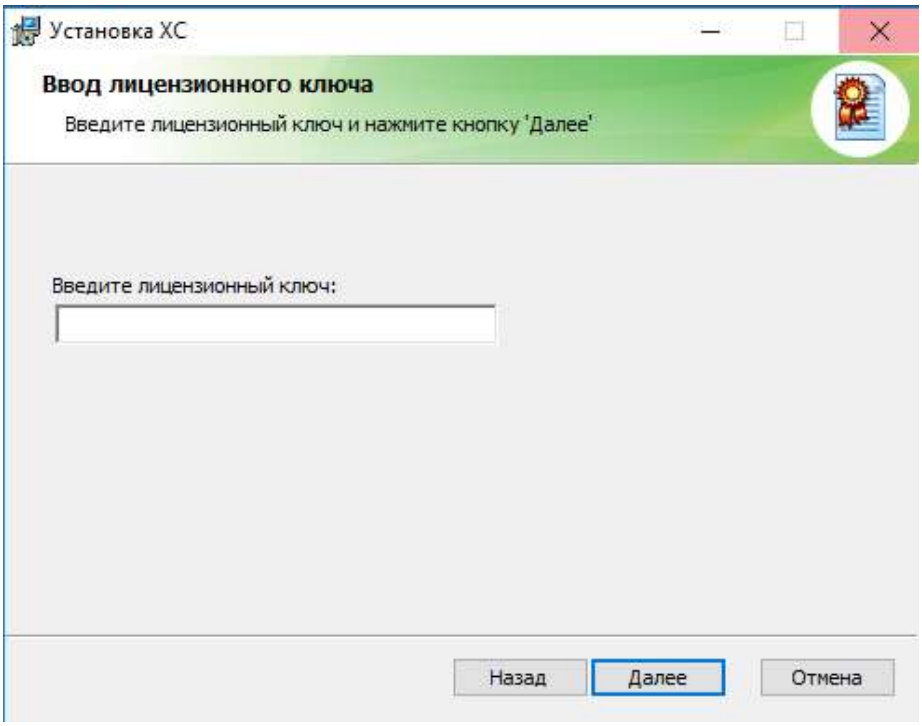


Рисунок 168 – Окно ввода лицензионного ключа

4) Введите лицензионный ключ и нажмите кнопку «Далее». Пользователю будет выведено информационное сообщение о готовности к установке опционального ПО "eXtended Container" (Рисунок 169).

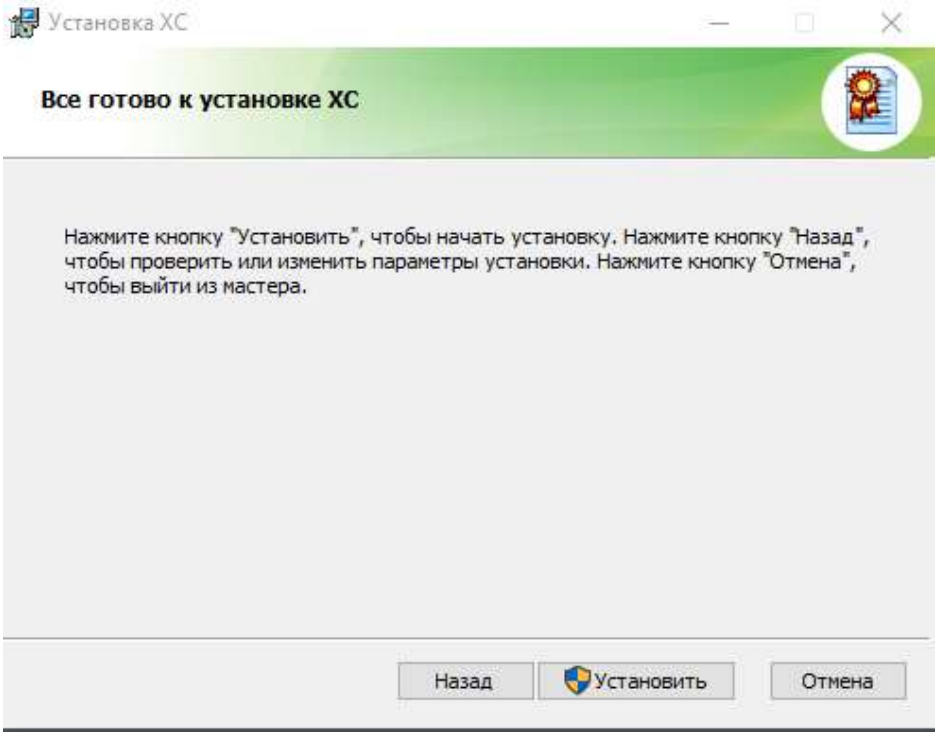


Рисунок 169 – Сообщение о готовности к установке "eXtended Container"

5) Нажмите кнопку «Установить». На экране отобразится диалог процесса установки опционального ПО "eXtended Container" (Рисунок 170).

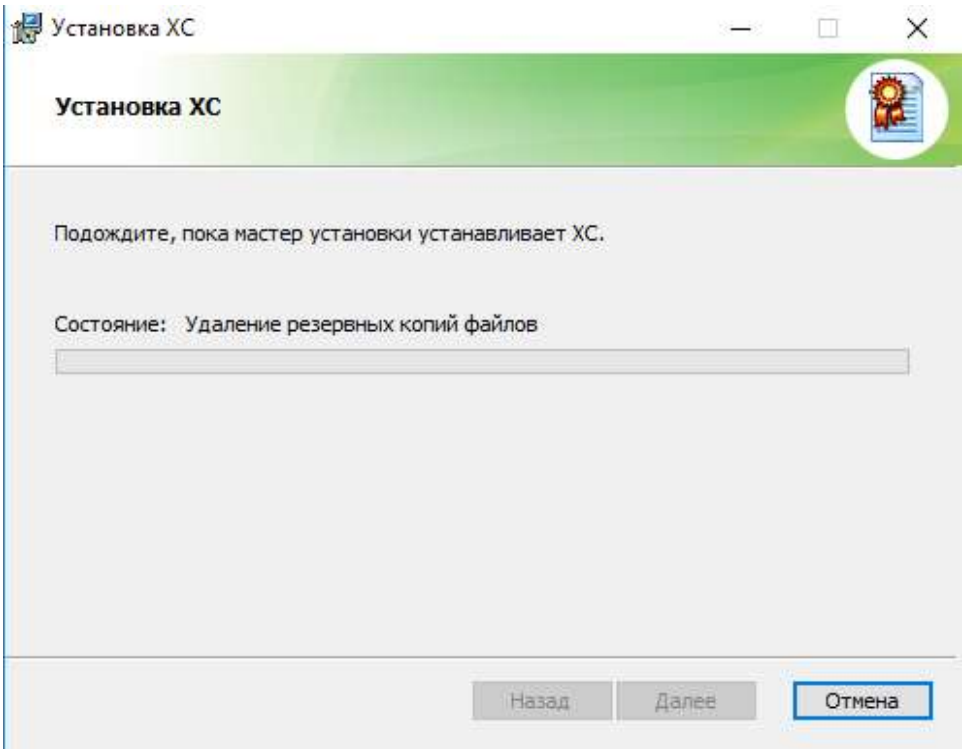


Рисунок 170 – Окно, информирующее пользователя о прогрессе установки опционального ПО "eXtended Container"

6) По завершению установки на экран будет выведен диалог об успешном завершении установки (Рисунок 171).

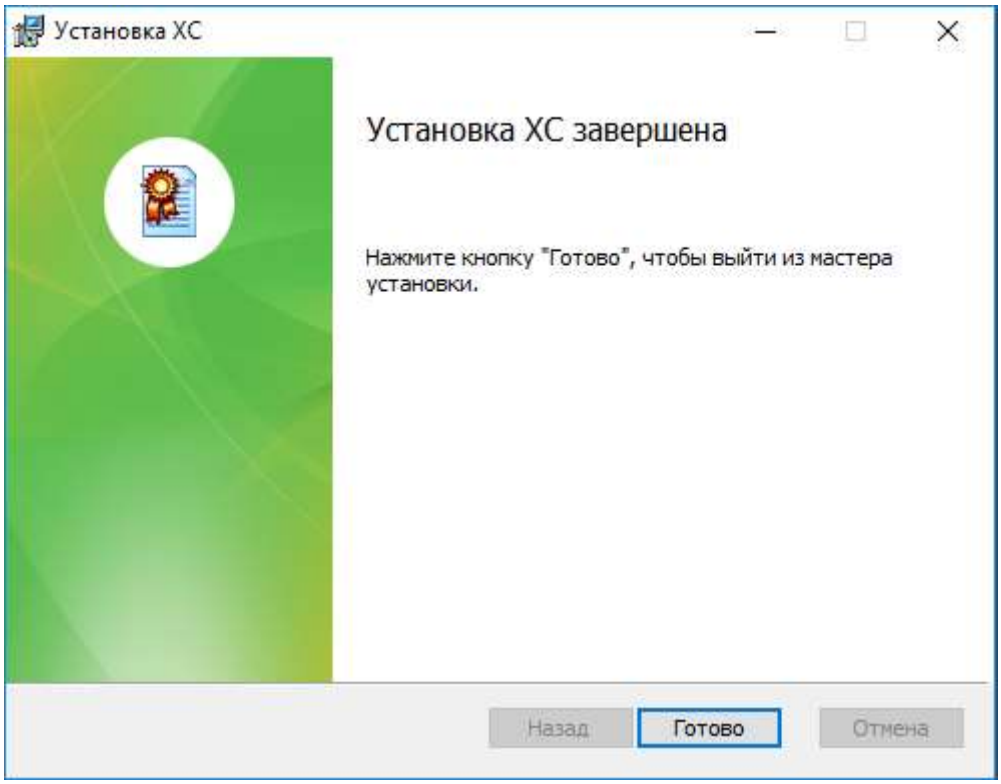


Рисунок 171 – Сообщение об успешном завершении установки опционального ПО "eXtended Container"

7) Нажмите кнопку «Готово». После установки опционального ПО "eXtended Container" дополнительных действий в части настройки данного ПО не требуется.

Б.2.13 Установка Jinn Sign Extension Provider

Jinn Sign Extension Provider необходим для взаимодействия с браузерами Google Chrome и Mozilla Firefox при вызове Jinn-Client.

В случае отсутствия дистрибутива необходимо обратиться в территориальный орган Федерального казначейства по месту нахождения. Также можно просмотреть порядок получения дистрибутивов на интернет-сайтах Управлений ФК в разделе ГИС > Удостоверяющий центр.

Рекомендуемая сборка Jinn Sign Extension Provider 1.1.0.5.

Для установки Jinn Sign Extension Provider необходимо:

1) Запустить файл установки. Откроется окно приветствия (Рисунок 172).

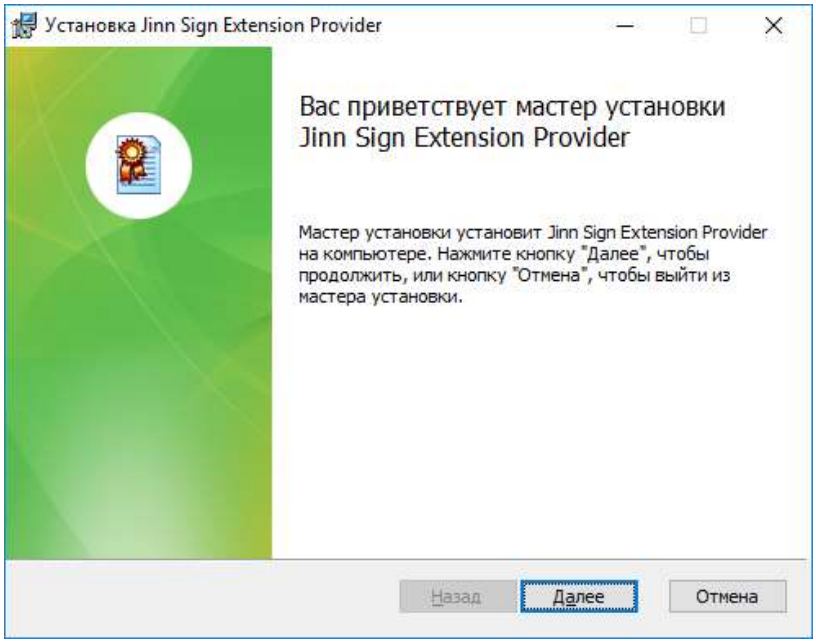


Рисунок 172 – Приветственное окно установки Jinn Sign Extension Provider

2) Нажать кнопку «Далее». Откроется окно «Лицензионного соглашения» (Рисунок 173). Отметить чекбокс «Я принимаю условия лицензионного соглашения».

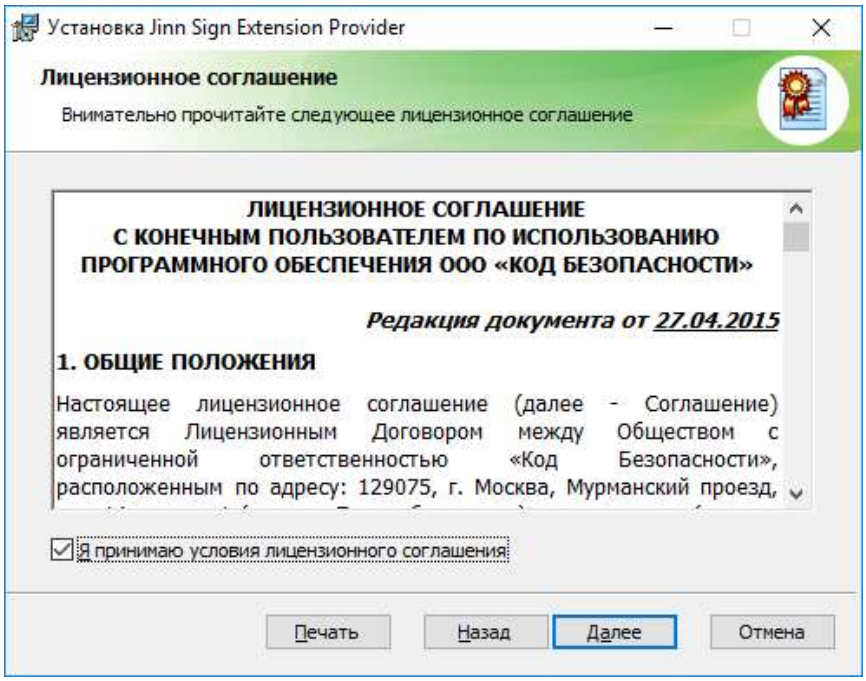


Рисунок 173 – Окно лицензионного соглашения Jinn Sign Extension Provider

3) Нажать кнопку «Далее». Откроется окно пути установки (Рисунок 174).

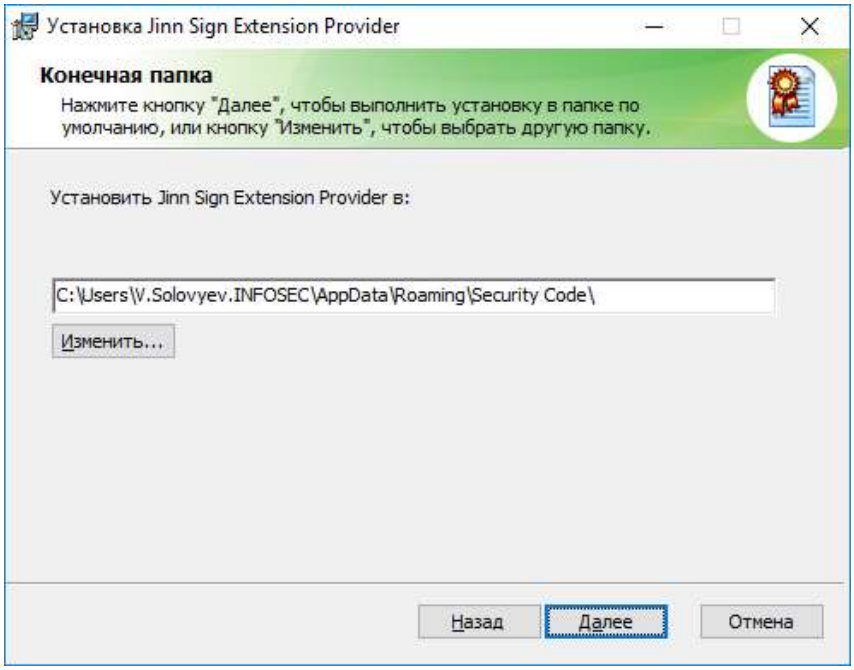


Рисунок 174 – Окно пути установки Jinn Sign Extension Provider

4) Нажать кнопку «Далее». Откроется окно установки (Рисунок 175).

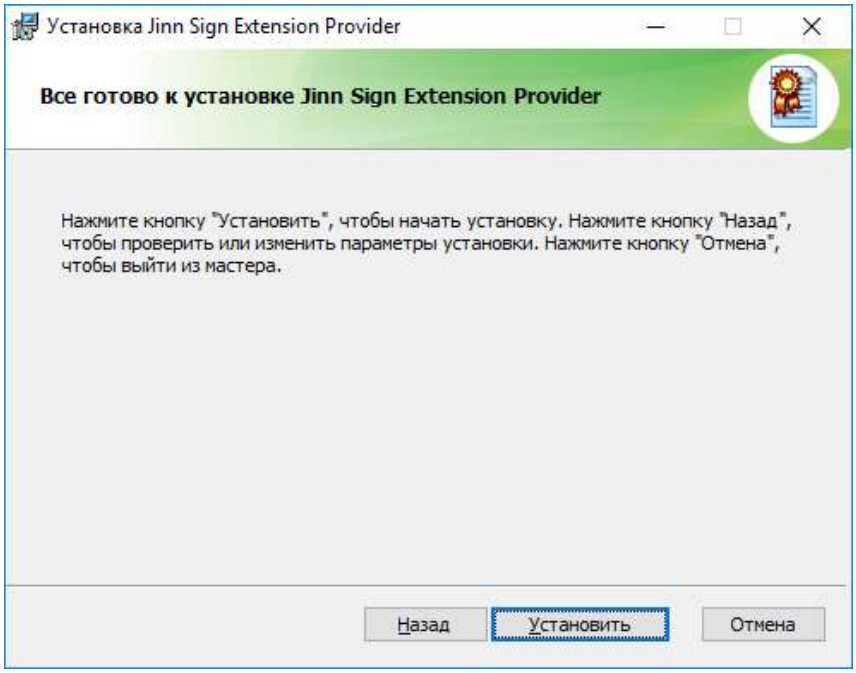


Рисунок 175 – Окно установки Jinn Sign Extension Provider

5) Нажать кнопку «Установить». Произведется установка провайдера и появится окно завершения установки (Рисунок 176).

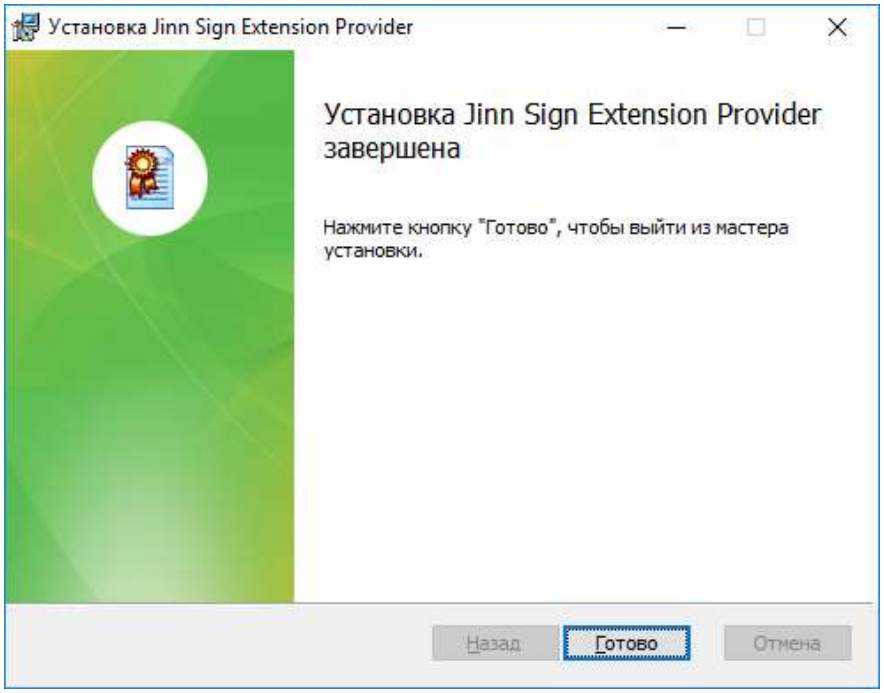


Рисунок 176 – Окно завершения установки Jinn Sign Extension Provider

6) Нажать кнопку «Готово». На этом установка Jinn Sign Extension Provider завершена.

Б.2.14 Установка расширения Jinn Sign Extension

Процесс установки расширения Jinn Sign Extension зависит от используемого веб-обозревателя (браузера):

1) Internet Explorer:

   Установка расширения не требуется.

2) Yandex:

   Для установки расширения Jinn Sign Extension для браузера Yandex необходимо:

   a) Открыть браузер Yandex;

   b) Открыть интернет-магазин chrome;

   c) Выполнить поиск расширения Jinn Sign Extension;

   d) Нажать «Установить» напротив найденного расширения;

   e) Подтвердить установку расширения в появившемся окне;

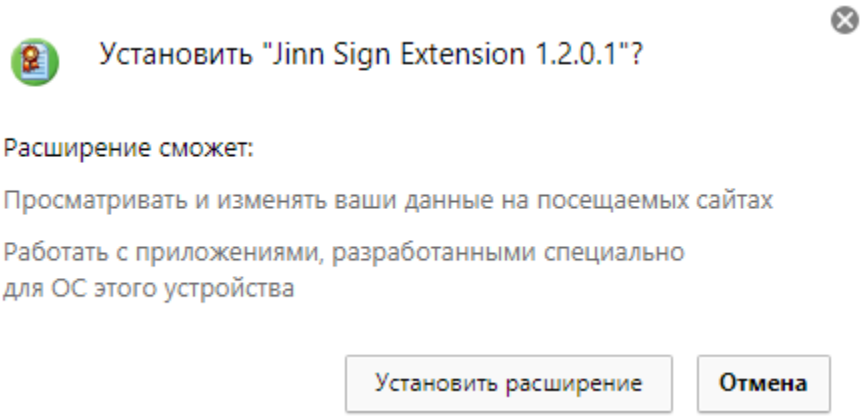


Рисунок 177 – Окно с подтверждением установки расширения Jinn Sign Extension

f) Отобразится уведомление о том, что расширение успешно установлено;

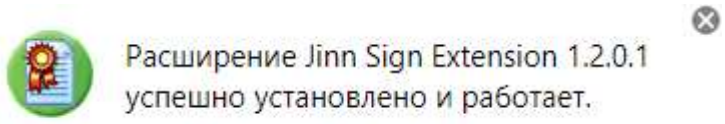


Рисунок 178 – Сообщение об успешном завершении установки расширения Jinn Sign Extension

g) Установка расширения Jinn Sign Extension для браузера Yandex на этом завершена.

После установки всех необходимых плагинов и расширений необходимо перезапустить используемый браузер и удостовериться, что все требуемые плагины и расширения включены.

Б.3 Перечень возможных ошибок при подключении к ПОИБ с применением СКЗИ «Континент TLS VPN Клиент»

Перечень возможных ошибок при подключении к подсистеме приведен в таблице 5. Сценарии устранения ошибок приведены в подразделе Б.4.

Таблица 5 – Перечень возможных ошибок при подключении

Описание ошибки	Раздел
403 Доступ запрещен «Не найден актуальный список отозванных сертификатов	Б.4.1
403 Доступ запрещен «Не найден корневой сертификат»	Б.4.2

Ошибка аутентификации: Учётная запись пользователя не найдена в системе. Обратитесь к Регистратору органа Федерального казначейства	Б.4.3
403 Доступ запрещен «Не выбран корректный сертификат клиента. Формат выбранного ключевого контейнера не поддерживается»	Б.4.4
503 Сервер назначения недоступен	Б.4.5
В окне выбора сертификата пользователя отсутствует требуемый сертификат	Б.4.6
Ошибка сертификата (400 The SSL certificate error): – сертификат имеет неправильное назначение; – сертификат отозван; – время действия сертификата еще не наступило; – сертификат истек.	Б.4.7

Б.4 Сценарии устранения ошибок

Б.4.1 403 Доступ запрещен «Не найден актуальный список отозванных сертификатов

1) Пройдите по адресу в сети Интернет: http://crl.roskazna.ru/crl/ucfk_2020.crl (или http://crl.roskazna.ru/crl/ucfk_gost12.crl).
2) Загрузите файл fk01.crl.
   a) Если файл fk01.crl недоступен к загрузке, то свяжитесь с администратором ЛВС своей Организации для выяснения причин невозможности перехода по указанному адресу.
3) Войдите в подсистему.
   a) Если при входе возникла ошибка «Не найден актуальный список отозванных сертификатов», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.2 403 Доступ запрещен «Не найден корневой сертификат»

1) Свяжитесь с Системным администратором своей Организации. Администратор установит корневой сертификат УЦ Федерального казначейства под учетной записью администратора в хранилище доверенных корневых центров сертификации локального компьютера.

   Администратор должен руководствоваться настоящим документом (пункт Б.2.5) при установке сертификата.
2) Войдите в подсистему.

a) Если при входе возникла ошибка «Не найден корневой сертификат», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.3 Ошибка аутентификации: Учётная запись пользователя не найдена в системе. Обратитесь к Регистратору своей организации

1) Свяжитесь с Регистратором своей Организации. Уточните статус выполнения заявки по регистрации вашей учетной записи или по импорту вашего сертификата пользователя.
2) При положительном ответе от Регистратора войдите в подсистему.
    a) Если при входе возникла ошибка с текстом «Ошибка аутентификации: Учётная запись пользователя не найдена в системе. Обратитесь к Регистратору органа Федерального казначейства», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.4 403 Доступ запрещен «Не выбран корректный сертификат клиента. Формат выбранного ключевого контейнера не поддерживается

1) Проверьте корректность выбранного сертификата: сертификат действителен, введен корректный пин-код (пароль) закрытого контейнера сертификата.
2) Войдите в подсистему.
    a) Если при входе возникла ошибка с текстом «403 Доступ запрещен «Не выбран корректный сертификат клиента. Формат выбранного ключевого контейнера не поддерживается», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.5 503 Сервер назначения недоступен

1) Свяжитесь с администратором ЛВС своей Организации. Администратор ЛВС дожен проверить доступность информационной системы *.cert.roskazna.ru по порту TCP-443 с рабочего АРМ Пользователя.
2) Войдите в подсистему.
    a) Если при входе возникла ошибка с текстом «503 Сервер назначения недоступен», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.6 В окне выбора сертификата пользователя отсутствует требуемый сертификат

1) Свяжитесь с Системным администратором своей Организации. Администратор или сам пользователь должен установить личный сертификат в хранилище Личных сертификатов. Администратор должен руководствоваться настоящим документом (пункт Б.2.6) при установке сертификата.
2) Штатными средствами ПО, на котором хранится ключевая информация сертификата пользователя (например, ПО eToken или Rutoken), убедитесь в корректности считывания сертификата пользователя.
    a) Если сертификат не считывается штатными средствами ПО, то выполните переустановку ПО носителя ключевой информации пользователя.
3) Войдите в подсистему.
    a) Если при входе возникла ошибка с текстом «В окне выбора сертификата пользователя отсутствует требуемый сертификат», то обратитесь в службу поддержки подсистемы и опишите ошибку.

Б.4.7 Ошибка сертификата

1) Убедитесь, что ваш сертификат пользователя подсистемы:
    — является действующим на момент работы в подсистеме;
    — выдан сертифицированным УЦ;
    — реквизитный состав сертификата пользователя является корректным для подсистемы.
2) Войдите в подсистеу.
    a) Если при входе возникла ошибка с текстом «Ошибка аутентификации: Учетная запись пользователя не найдена в системе. Обратитесь к Регистратору органа Федерального казначейства», то обратитесь в службу поддержки подсистемы и опишите ошибку. К обращению в обязательном порядке должен быть приложен сертификат УЦ, которым подписан сертификат пользователя (необходимо обратиться в УЦ, в котором был выдан сертификат пользователя), а также скриншот окна браузера с ошибкой входа.