Федеральная государственная информационная система ценообразования в строительстве (ФГИС ЦС)

Инструкция по входу в личный кабинет ФГИС ЦС

2017

Аннотация

Уважаемые пользователи ФГИС ЦС!

Данная инструкция описывает порядок получения доступа к личному кабинету ФГИС ЦС и предназначена для:

1) производителей строительных ресурсов на территории Российской Федерации;
2) организаций, осуществляющих ввоз этих ресурсов в Российскую Федерацию для внутреннего потребления;
3) перевозчиков строительных ресурсов;
4) собственников грузовых вагонов,

которые в соответствии с постановлением Правительства Российской Федерации от 23.12.2016 №1452 должны вносить сведения об отпускных ценах строительных ресурсов и услугах по их перевозке.

Содержание

Перечень терминов и сокращений

Термин, сокращение	Определение
CRL	Список аннулированных сертификатов SSL
SSL	Криптографический протокол, который подразумевает безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений
ГОСТ	Государственный стандарт
ЕСИА	Единая система идентификации и аутентификации, предназначена для формирования единых методов регистрации, идентификации и аутентификации пользователей во всех государственных информационных системах
Корневой сертификат УКЭП	Сертификат Удостоверяющего центра, полученный в комплекте с усиленной квалифицированной электронной подписью (сертификат издателя пользовательского сертификата)
Минкомсвязь России	Министерство связи и массовых коммуникаций Российской Федерации
ПО «Jinn-Client»	Сертифицированное средство криптографической защиты информации для создания электронной подписи и доверенной визуализации документов
ПО	Программное обеспечение
ПО «Континент TLS VPN»	Средство криптографической защиты информации, система обеспечения защищенного удаленного доступа к web-приложениям с использованием алгоритмов шифрования ГОСТ
Портал Госуслуг	Портал государственных услуг Российской Федерации
Портал ФГИС ЦС	Подсистема Портал федеральной государственной информационной системы ценообразования в строительстве
Постановление Правительства Российской Федерации от 23.12.2016 №1452	Постановление Правительства Российской Федерации от 23.12.2016 №1452 «О мониторинге цен строительных ресурсов»
ФГИС ЦС	Федеральная государственная информационная система ценообразования в строительстве
Сертификат пользователя	Сертификат пользователя, полученный в комплекте с усиленной квалифицированной электронной подписью и подтверждающий принадлежность ключа проверки электронной подписи конкретному владельцу
Сертификат сервера	Сертификат сервера для ПО «Континент TLS VPN», ранее полученный на Портале ФГИС ЦС в разделе «База знаний» в подразделе «Обучающие материалы» (файл **fgiscs-tls.gge.ru (1).cer**)

Термин, сокращение	Определение
Сертификат Удостоверяющего центра	Сертификат Удостоверяющего центра для ПО «Континент TLS VPN», ранее полученный на Портале ФГИС ЦС в разделе «База знаний» в подразделе «Обучающие материалы» (файл **уц иит т1 (1).cer**)
СНИЛС	Страховой номер лицевого счета гражданина в системе обязательного пенсионного страхования
УКЭП	Усиленная квалифицированная электронная подпись

1 Общие положения

Для входа на Портал ФГИС ЦС сначала получите УКЭП (см. п. 2), которая понадобится для создания учетной записи организации на портале Госуслуг, а также для обеспечения юридической значимости передаваемых во ФГИС ЦС данных, и пройдите авторизацию на портале Госуслуг.

Для регистрации организации (см. п. 4) сначала зарегистрируйте физическое лицо (руководителя организации либо представителя организации, имеющего право действовать от имени организации без доверенности) (см. п. 3).

2 Порядок получения УКЭП

Для полноценной работы в личном кабинете ФГИС ЦС, подключение к которому осуществляется по ссылке https://fgiscs-tls.gge.ru:8443, пользователь должен получить УКЭП в аккредитованном Удостоверяющем центре. Для получения средства УКЭП обратитесь в один из аккредитованных Минкомсвязью России Удостоверяющих центров, указанных на сайте minsvyaz.ru/ru/activity/govservices/2, следуя инструкциям сайта minsvyaz.ru/ru/appeals/faq/35.

В комплект УКЭП входят:

1) сертификат пользователя (электронный документ, выданный аккредитованным Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи конкретному владельцу). Порядок установки сертификата пользователя описан ниже (см. п. 7);
2) криптоконтейнер, размещенный на внешнем носителе;
3) пароль криптоконтейнера (набор символов в бумажном или электронном виде);
4) корневой сертификат УКЭП. Порядок установки корневого сертификата УКЭП описан ниже (см. п. 5).

Внешний носитель должен соответствовать рекомендованным типам:

- USB флеш-накопитель;
- USB-ключ Rutoken S;
- USB-ключ eToken Pro;
- USB-ключ eToken PRO (Java).

При использовании носителя информации Rutoken S должен быть установлен соответствующий драйвер, который доступен для загрузки по ссылке ниже: rutoken.ru/support/download/drivers-for-windows.

При использовании носителя информации eToken установите набор драйверов, доступный по ссылке aladdin-rd.ru/support/downloads/38524 или aladdin-rd.ru/support/downloads/26037 и единый клиент «JaCarta», доступный для загрузки по адресу aladdin-rd.ru/support/downloads/43987.

В случае если полученный в Удостоверяющем центре тип носителя криптоконтейнера не соответствует ни одному из рекомендованных, достаточно при помощи криптопровайдера перенести закрытый ключ на поддерживаемый тип носителя. Получение нового ключа УКЭП не требуется.

3 Порядок регистрации физического лица

Для регистрации физического лица выполните следующую последовательность действий:

1) приготовьте паспорт и страховое свидетельство обязательного пенсионного страхования;
2) перейдите на портал Госуслуг – откройте страницу регистрации на esia.gosuslugi.ru/registration/;
3) заполните поля: «Фамилия», «Имя», «Мобильный телефон» или «Или электронная почта», нажмите кнопку «Зарегистрироваться»;
4) подтвердите номер телефона или адрес электронной почты. В результате на адрес электронной почты будет выслан код подтверждения;
5) откройте электронное письмо и перейдите по указанной в нем ссылке подтверждения;
6) после уведомления о завершенной регистрации портал Госуслуг перенаправит пользователя на форму заполнения личных данных. Будьте внимательны при заполнении формы личных данных. Отправьте их на автоматическую проверку, нажав кнопку «Сохранить»;
7) нажмите кнопку «Заполнить профиль» и введите данные для создания стандартной учетной записи. Указанные личные данные отправятся на автоматическую проверку в Пенсионный Фонд Российской Федерации и Главное управление по вопросам миграции Министерства внутренних дел Российской Федерации. После завершения процедуры проверки придет соответствующее уведомление;
8) выполните процедуру подтверждения личности – эта процедура предусматривает ввод персонального идентификатора, полученного лично одним из следующих доступных способов:
   - первый способ – *личное обращение*. Предполагает посещение специализированного центра обслуживания. Потребуется предъявить документ, который был указан на этапе ввода личных данных, и СНИЛС. Найти ближайшие центры подтверждения личности можно, перейдя по ссылке «Найти центр обслуживания». Центры подтверждения личности на карте будут обозначены точками. Нажмите на точку для получения информации о режиме работе выбранного центра;
   - второй способ – *через Почту России*. В этом случае письмо с кодом подтверждения личности будет выслано на почтовый адрес. Код высылается заказным письмом. Потребуется предъявить документ, удостоверяющий

личность, и извещение. Если данный способ подтверждения личности подходит, выберите в меню на портале Госуслуг параметр «Заказным письмом почтой России».

Если код подтверждения личности введен и успешно проверен, станет доступна услуга регистрации юридического лица, а на странице личного кабинета появится отметка о наличии подтвержденной учетной записи.

9) перейдите к регистрации юридического лица (см. п. 4).

4 Порядок регистрации юридического лица

Порядок регистрации юридического лица:

1) авторизуйтесь на портале Госуслуг (esia.gosuslugi.ru) под учетной записью физического лица и нажмите кнопку «Показать все личные данные» на вкладке «Персональная информация». Следует учитывать, что для создания учетной записи организации необходимо предварительное наличие средства УКЭП юридического лица;
2) подключите к компьютеру средство электронной подписи;
3) убедитесь, что в качестве типа организации выбран параметр «Юридическое лицо». Далее укажите ряд дополнительных сведений об организации и ее руководителе. Дождитесь результатов автоматической проверки данных в Федеральной налоговой службе. До окончания проверки можно закрыть данную страницу, при необходимости ход выполнения проверки можно просмотреть через личную страницу ЕСИА. Информация о результате проверки поступит пользователю в виде уведомления в личном кабинете на портале ЕСИА;
4) затем при входе во ФГИС ЦС в качестве юридического лица может появиться запрос роли. В этом случае выберите организацию, от имени которой предполагается работать в ЕСИА;
5) для отправки приглашения пользователю нажмите на странице со списком сотрудников кнопку «Пригласить нового участника». Отобразится страница приглашения сотрудника. Заполните обязательные поля ввода адреса электронной почты и фамилии, имени, отчества. Будьте внимательны при заполнении полей. Для назначения сотрудника администратором выберите параметр «Администраторы профиля организации». Затем нажмите на кнопку «Пригласить». Сотруднику на указанный адрес электронной почты поступит письмо со ссылкой. После того как сотрудник воспользуется ссылкой и авторизуется в ЕСИА, он будет присоединен к организации.

Для передачи данных в ФГИС ЦС юридическому лицу дополнительно требуется установить специальные программы: ПО «Jinn-Client» (см. п. 15)) и ПО «Континент TLS VPN» (см. п. 6.1).

5 Порядок установки корневого сертификата УКЭП

Установите корневой сертификат УКЭП до установки и настройки ПО «Континент TLS VPN» и ПО «Jinn-Client».

Для установки корневого сертификата УКЭП выполните следующие действия (только от имени пользователя, входящего в группу локальных администраторов):

1) в меню «Пуск» выберите команду «Выполнить». В открывшемся окне введите команду «mmc» (Рисунок 1), нажмите на кнопку «ОК»;

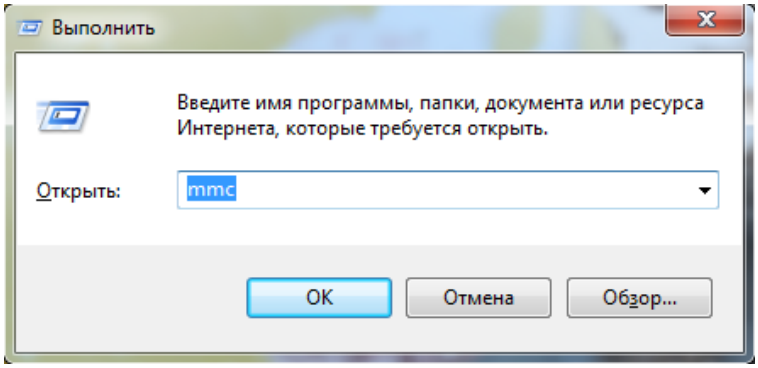

Рисунок 1 – Окно «Выполнить»

2) откроется окно подтверждения запуска приложения, нажмите на кнопку «Да». Откроется консоль управления (Рисунок 2);

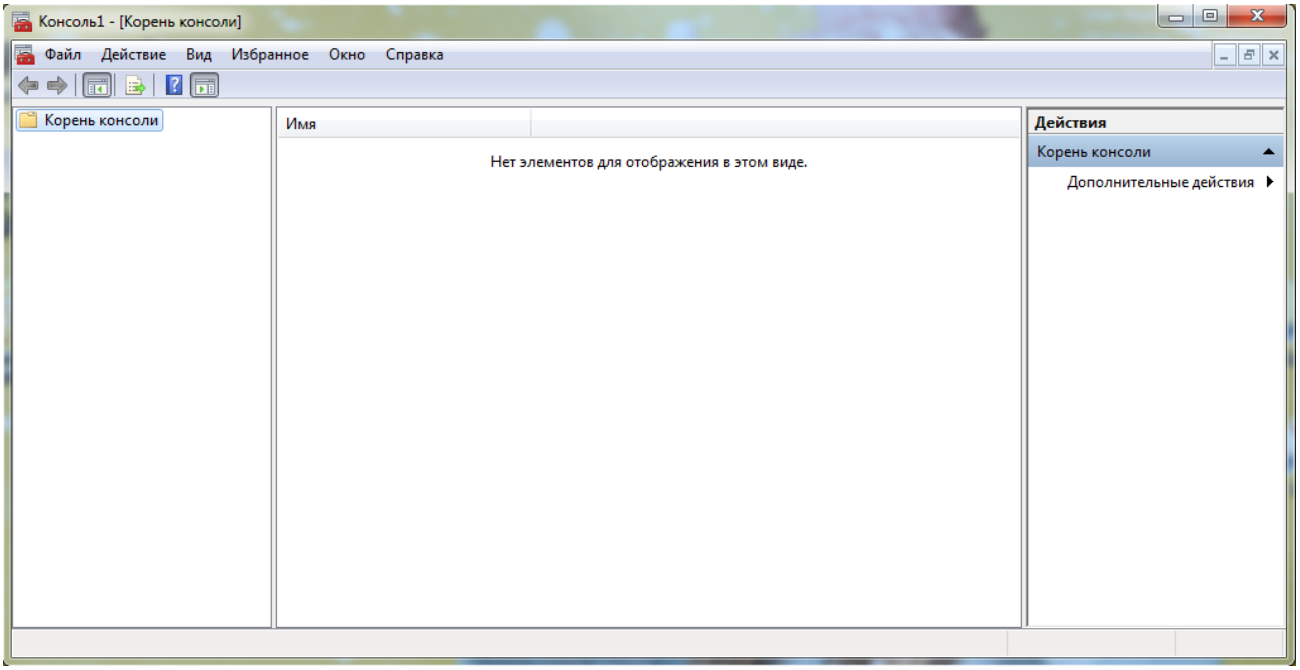

Рисунок 2 – Консоль управления

3) в консоли управления выберите пункт «Файл/Добавить или удалить оснастку». Откроется окно «Добавление и удаление оснасток» (Рисунок 3);

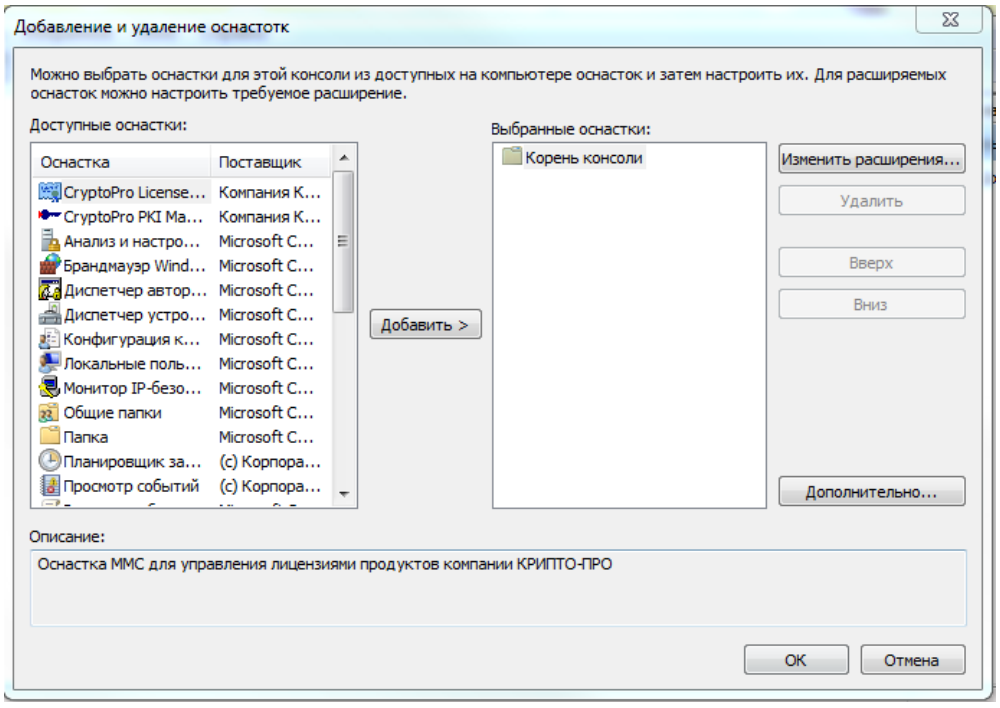

Рисунок 3 – Окно «Добавление и удаление оснасток»

4) в открывшемся окне в области «Доступные оснастки» выделите оснастку «Сертификаты» и нажмите кнопку «Добавить» (Рисунок 4);

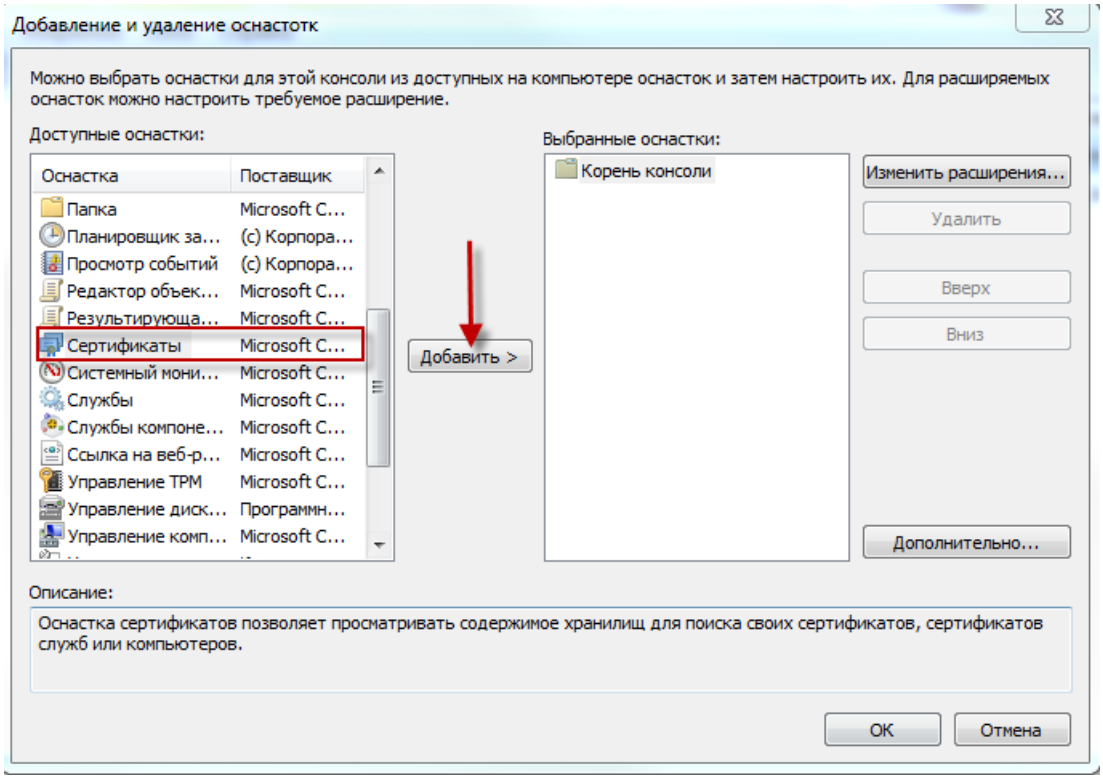

Рисунок 4 – Окно «Добавление и удаление оснасток». Кнопка «Добавить»

5) в открывшемся диалоговом окне установите «флажок» в поле «учетной записи компьютера» и нажмите кнопку «Далее» (Рисунок 5);

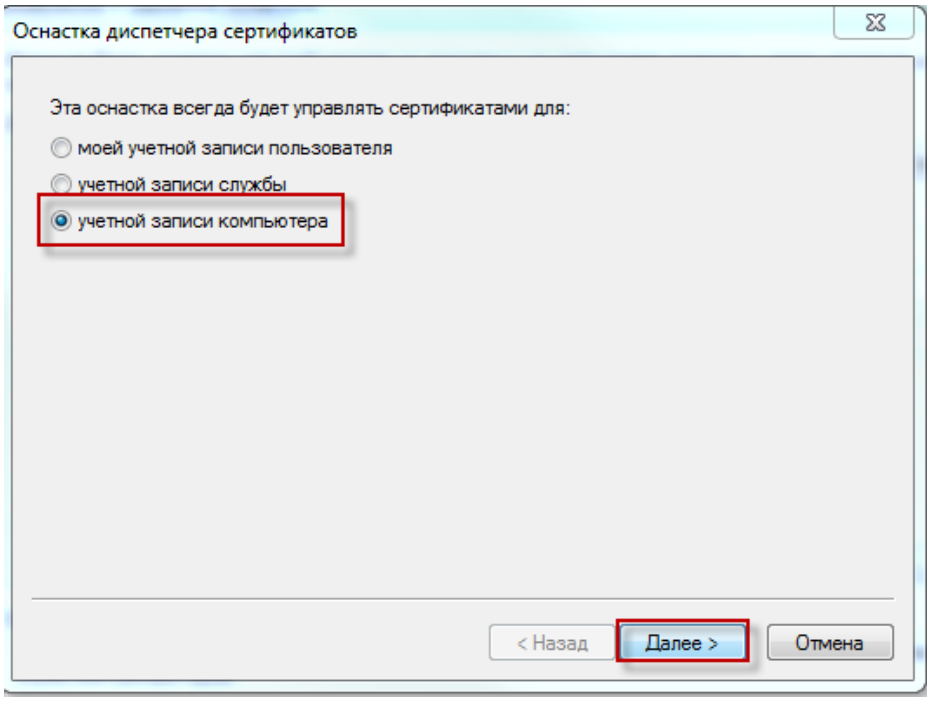

Рисунок 5 – Окно оснастки диспетчера сертификатов

6) в открывшемся окне установите «флажок» в поле «локальным компьютером» и нажмите на кнопку «Готово» (Рисунок 6);

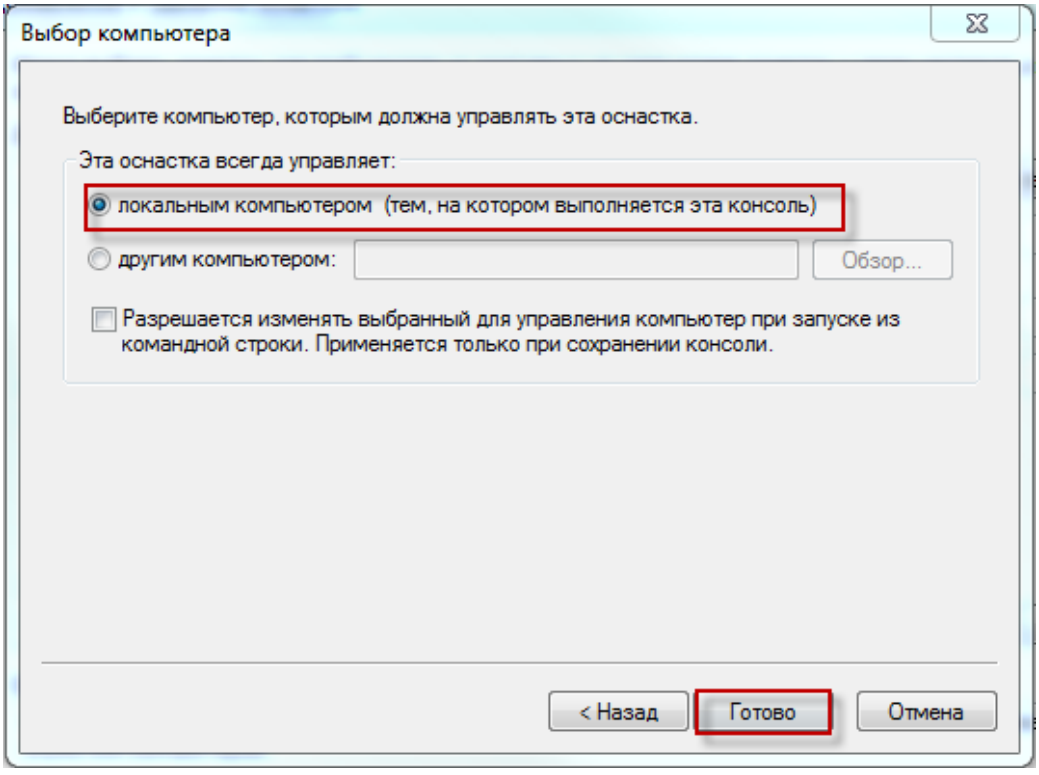

Рисунок 6 – Окно выбора компьютера

7) в окне «Добавление и удаление оснасток» нажмите на кнопку «Ок» (Рисунок 7);

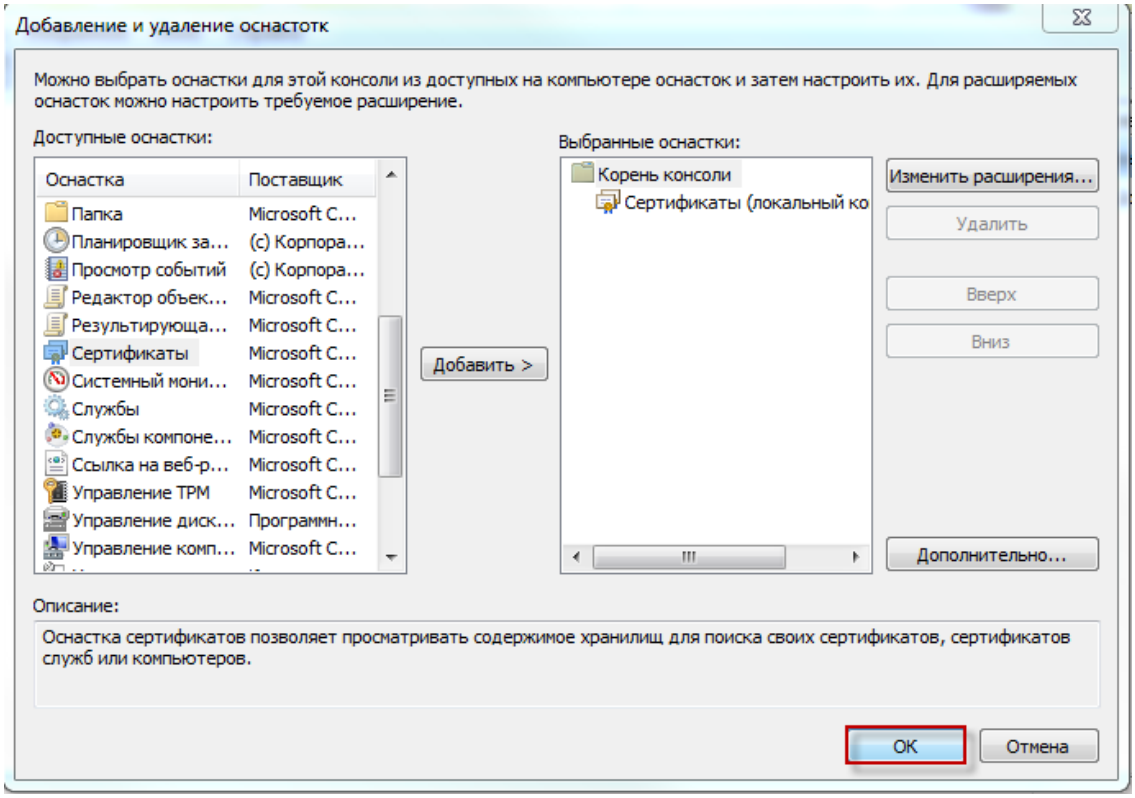

Рисунок 7 – Окно добавления и удаления оснасток

8) в консоли управления будет отображаться закладка «Сертификаты (локальный компьютер)». Раскройте ее нажатием кнопки ▷ (Рисунок 8);

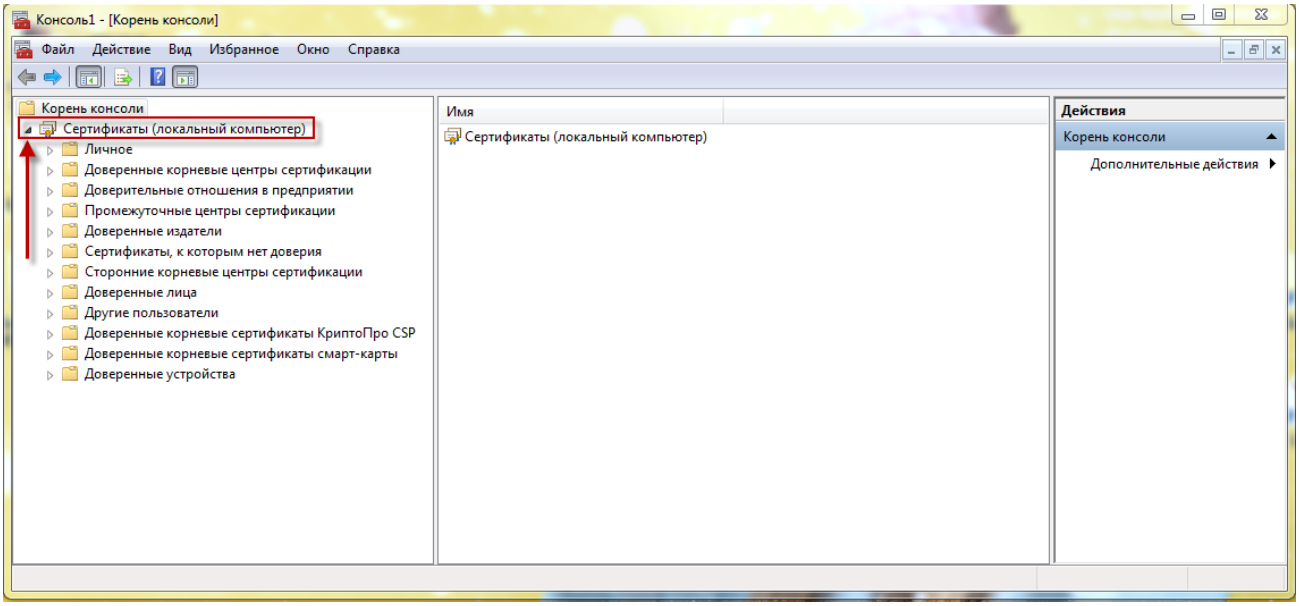

Рисунок 8 – Окно консоли

9) раскройте папку «Доверенные корневые центры сертификации», нажмите правой кнопкой мыши на папку «Сертификаты» и выберите пункт «Все задачи/Импорт» (Рисунок 9);

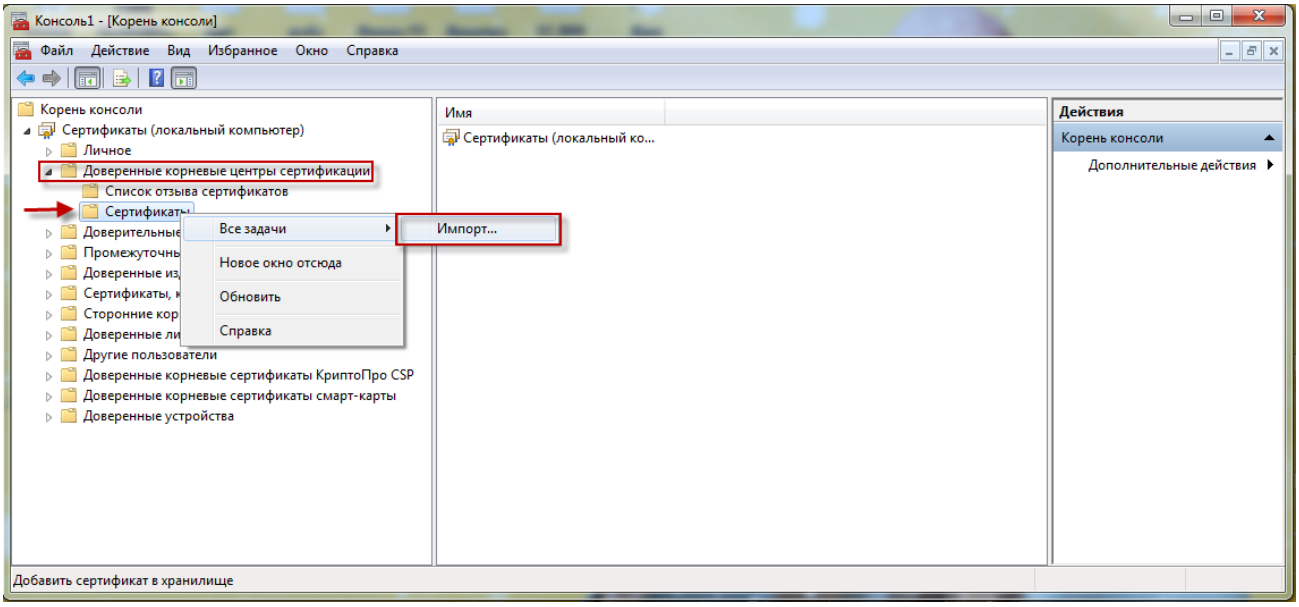

Рисунок 9 – Окно консоли

10) откроется окно «Мастер импорта сертификата», для импорта сертификата нажмите кнопку «Далее» (Рисунок 10);

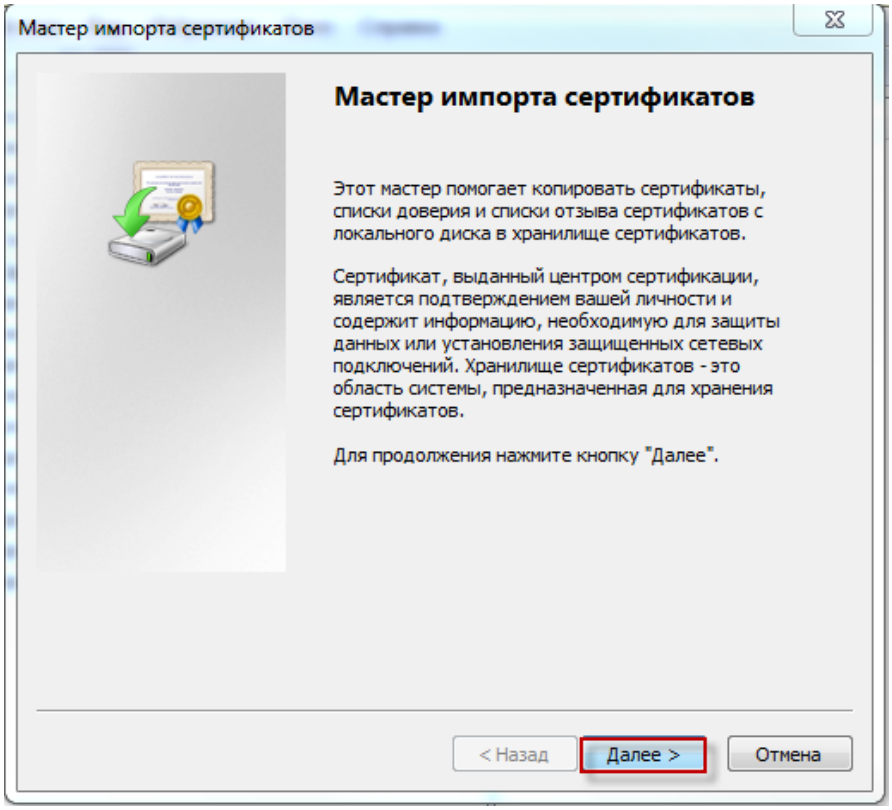

Рисунок 10 – Окно Мастера импорта сертификатов. Шаг 1

11) нажмите на кнопку «Обзор» для выбора корневого сертификата УКЭП (Рисунок 11);

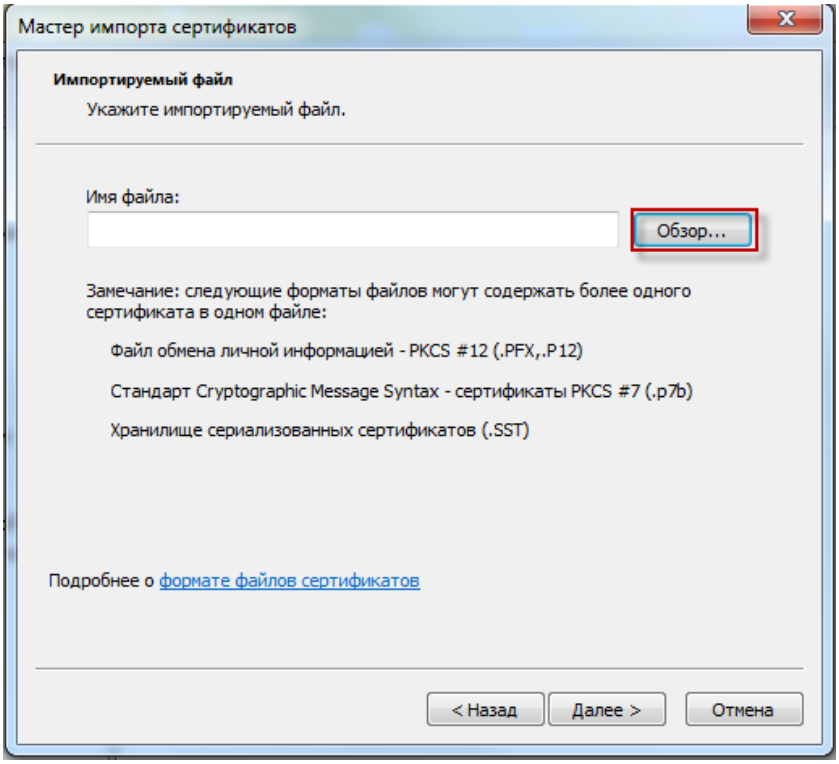

Рисунок 11 – Окно Мастера импорта сертификатов. Шаг 2

12) в окне выбора сертификата откройте папку, в которой лежит корневой сертификат УКЭП, выделите его и нажмите на кнопку «Открыть» (Рисунок 12);

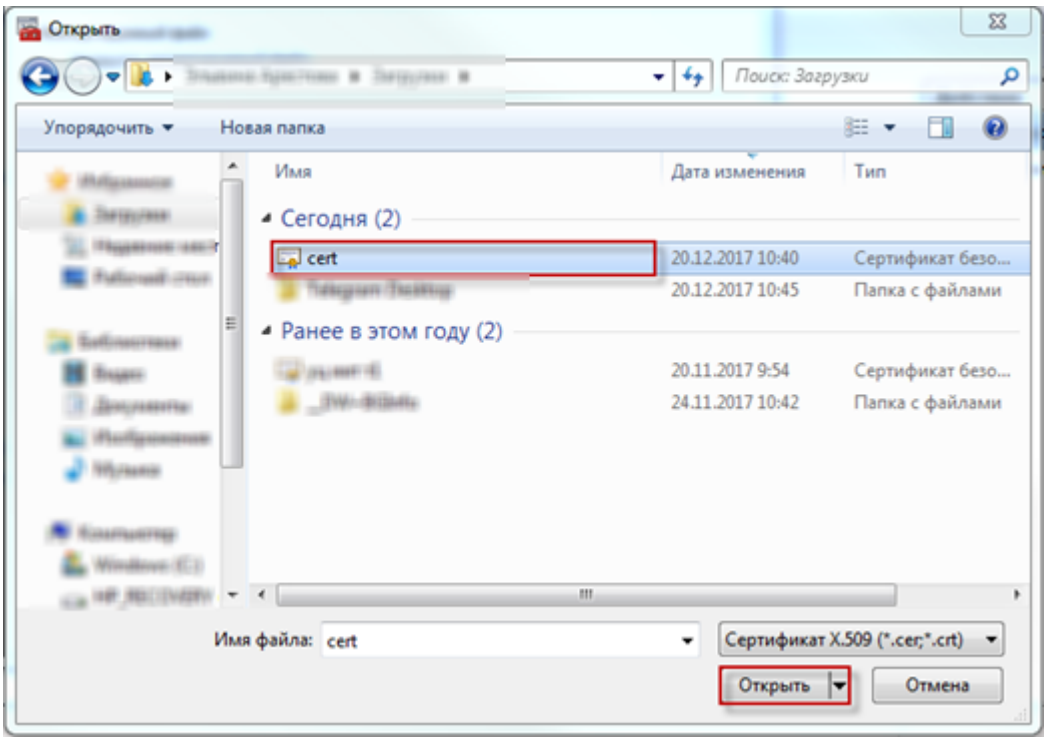

Рисунок 12 – Окно выбора корневого сертификата УКЭП

13) в окне «Мастер импорта сертификатов» нажмите кнопку «Далее». В окне выбора хранилища сертификатов, не внося изменений, нажмите на кнопку «Далее» (Рисунок 13);

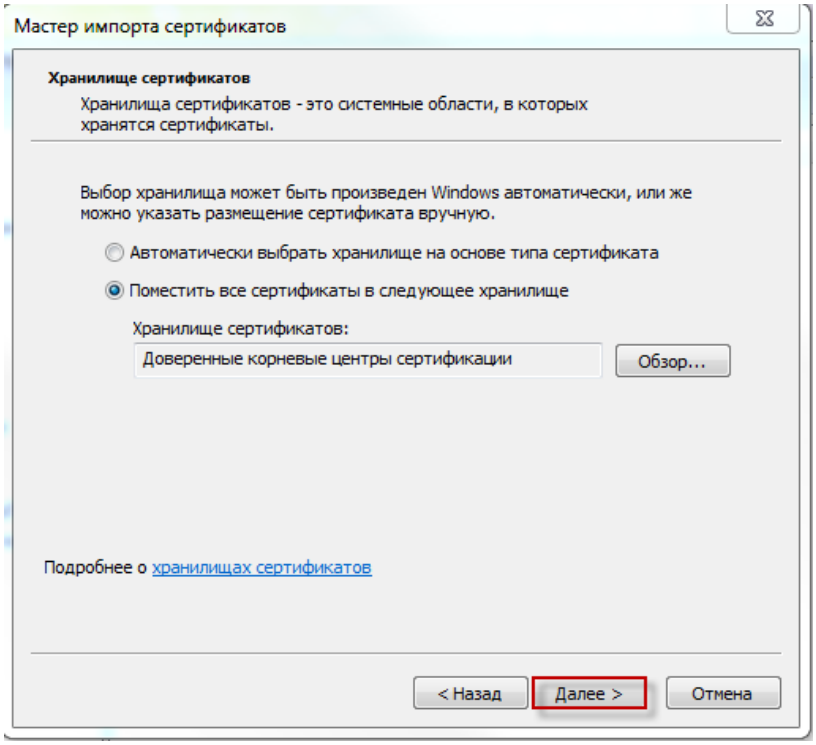

Рисунок 13 – Окно Мастера импорта сертификатов. Шаг 3

14) в окне завершения мастера импорта сертификатов нажмите на кнопку «Готово» (Рисунок 14);

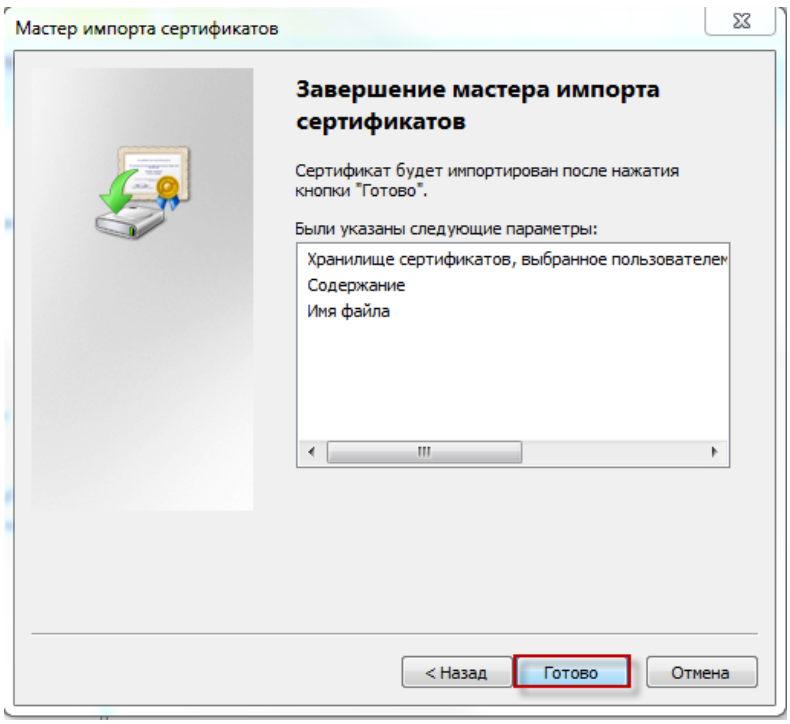

Рисунок 14 – Окно Мастера импорта сертификатов. Шаг 4

15) откроется окно с сообщение о том, что импорт корневого сертификата УКЭП выполнен успешно. Нажмите кнопку «Ок» (Рисунок 15).

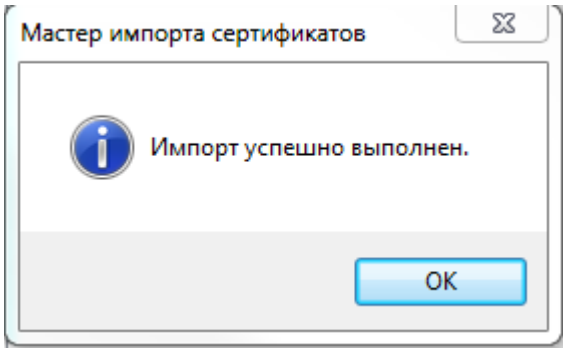

Рисунок 15 – Сообщение о выполнении импорта корневого сертификата УКЭП

Примечание – При закрытии окна консоли, откроется окно с сообщением: «Сохранить параметры в консоли в «Консоль1?». Нажмите на кнопку «Нет» (Рисунок 16).

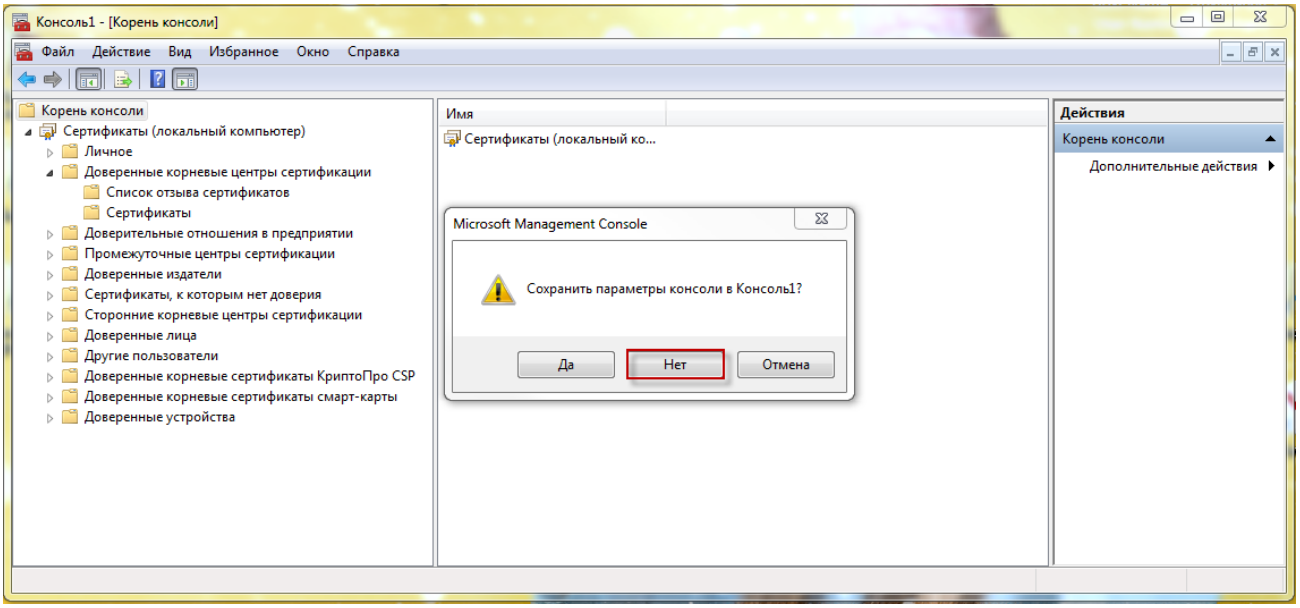

Рисунок 16 – Закрытие окна консоли

Установка корневого сертификата УКЭП завершена.

6 Установка ПО «Jinn-Client»

Для установки ПО «Jinn-Client» выполните следующую последовательность действий:

1) поместите установочный диск в устройство чтения компакт-дисков и запустите к исполнению файл «Setup» (Рисунок 17);

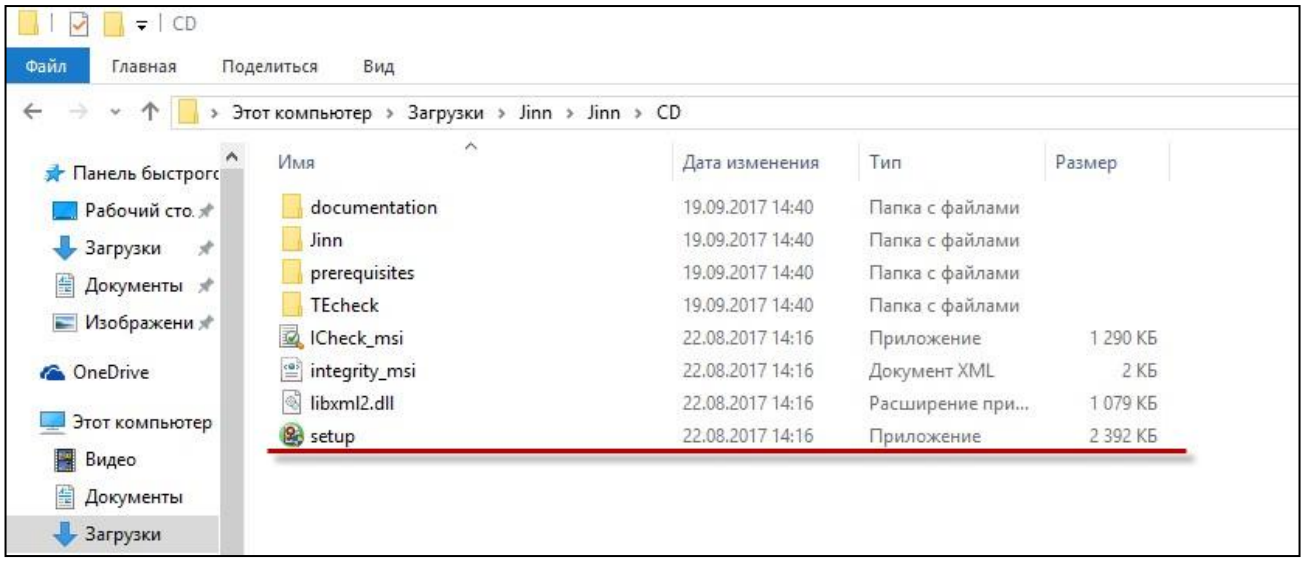

Рисунок 17 – Файл «Setup»

2) на экране отобразится окно с выбором компонентов. Выберите пункт «Jinn-Client» (Рисунок 18);

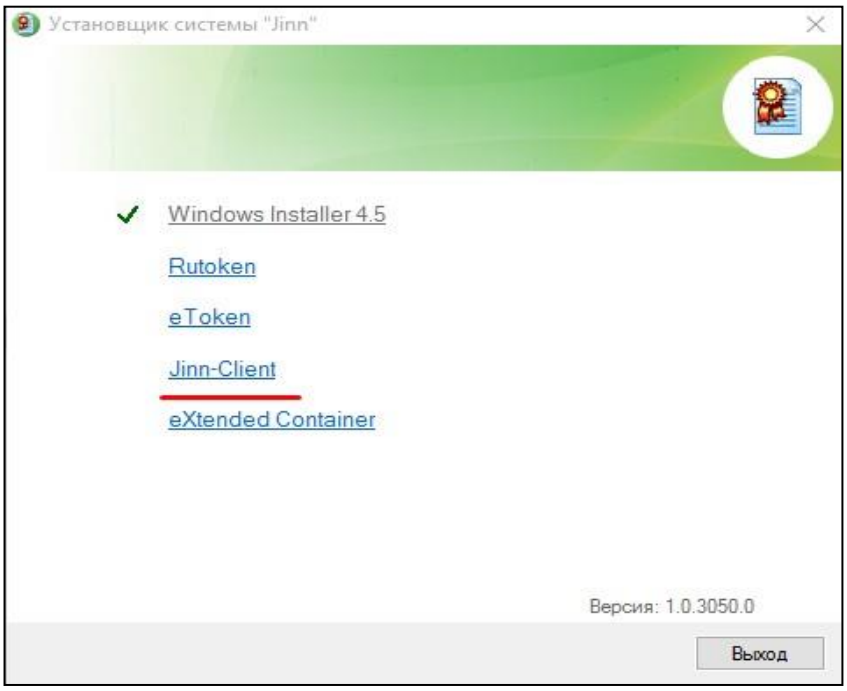

Рисунок 18 – Пункт «Jinn-Client»

3) в окне «Установка Jinn-Client» нажмите кнопку «Далее» (Рисунок 19);

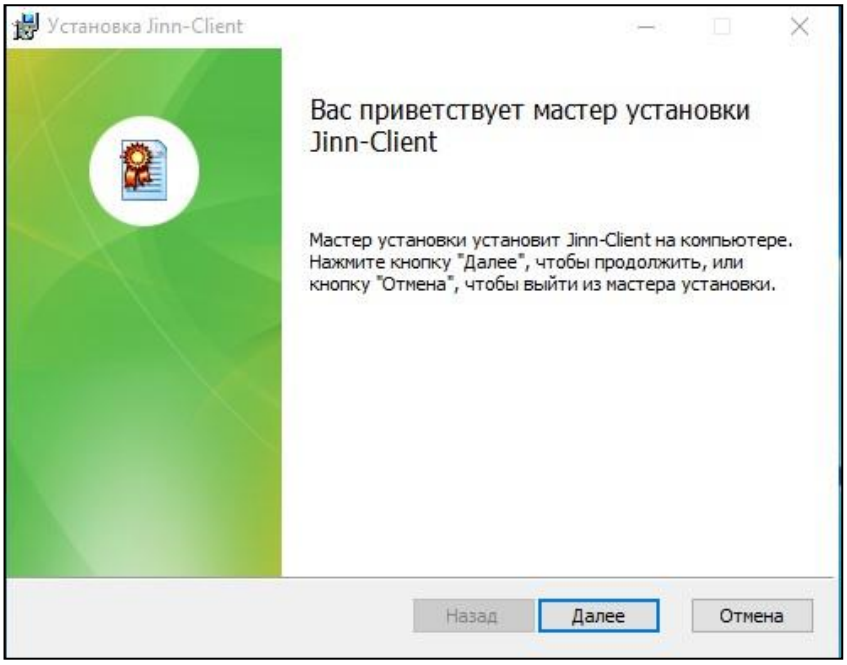

Рисунок 19 – Окно «Установка Jinn-Client»

4) отобразится лицензионное соглашение (Рисунок 20). Ознакомьтесь с ним, установите «флажок» в поле «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее»;

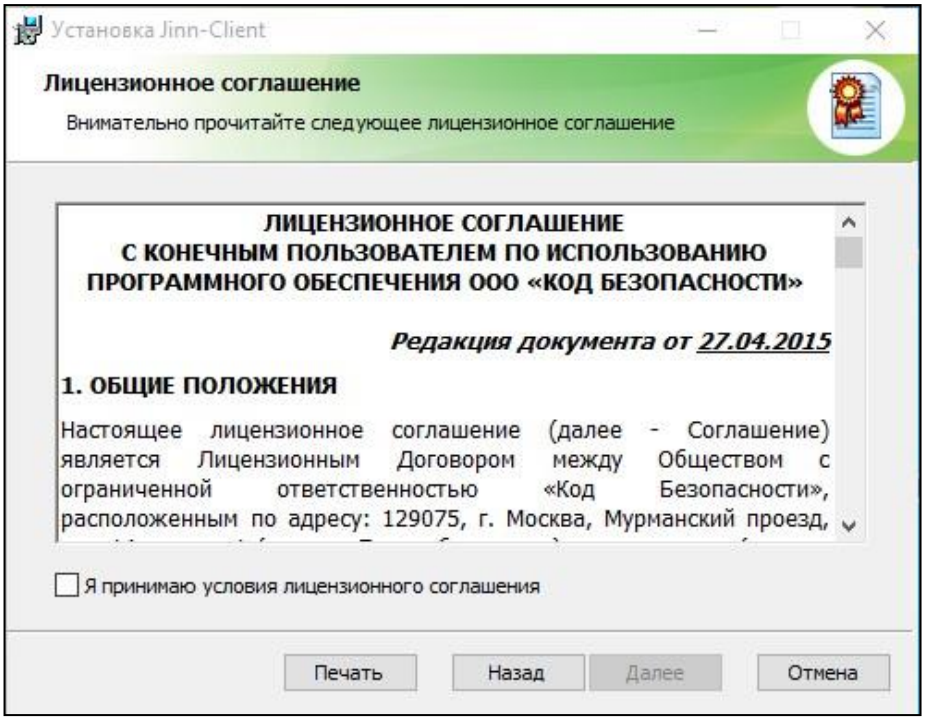

Рисунок 20 – Лицензионное соглашение

5) в окне «Ввод лицензионного ключа» (Рисунок 21) введите номер лицензионного ключа и нажмите кнопку «Далее»;

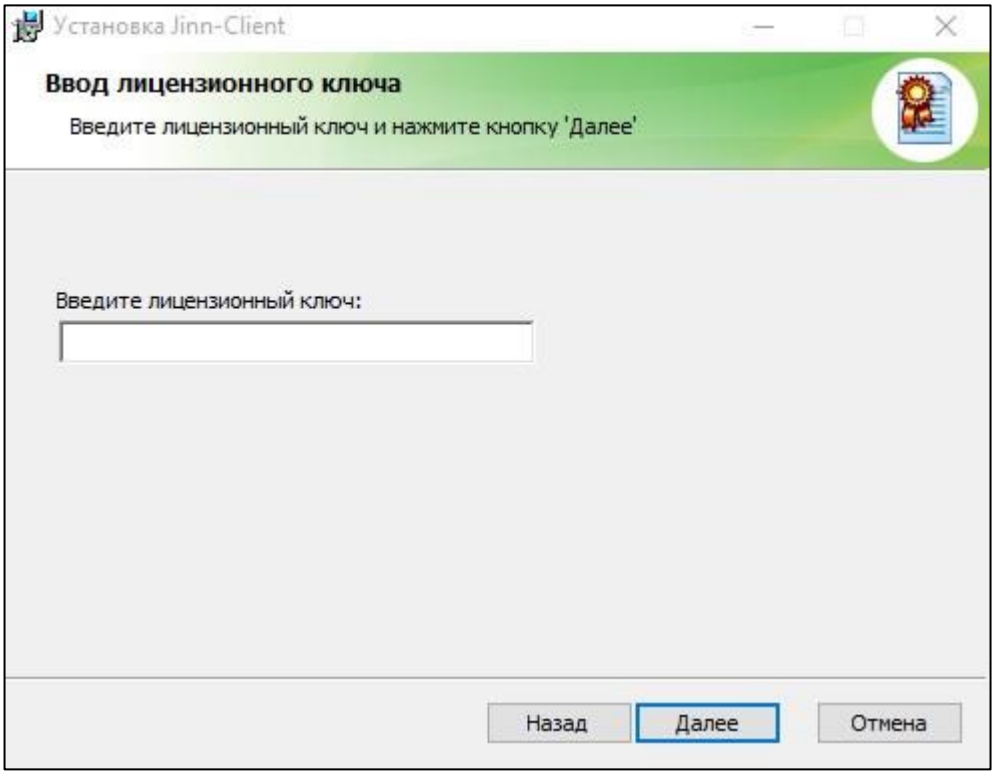

Рисунок 21 – Окно «Ввод лицензионного ключа»

6) в следующем окне установщиком будет предложено расположение каталога локального компьютера для разворачивания в нем ПО «Jinn-Client». Согласитесь с предложенным расположением, нажав кнопку «Далее» (Рисунок 22);

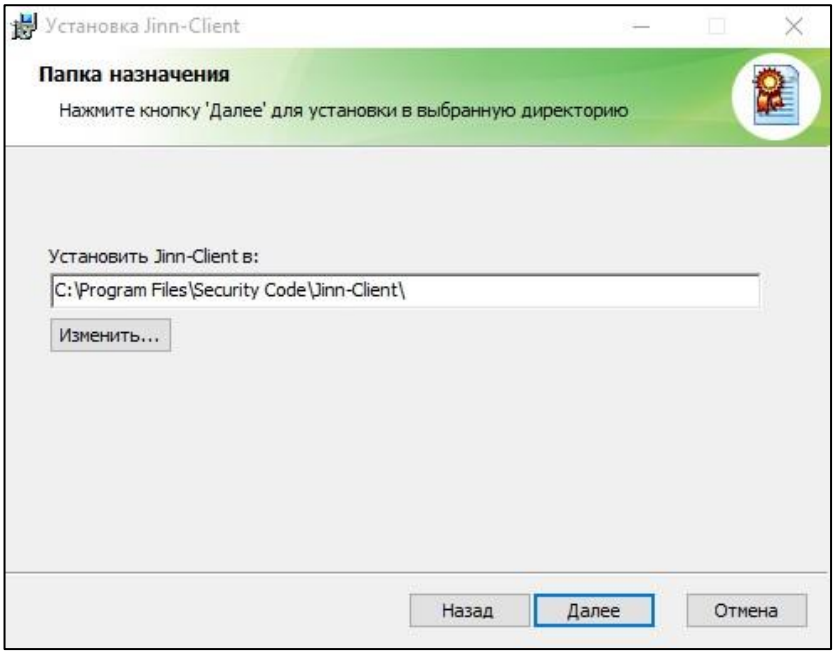

Рисунок 22 – Расположение каталога для разворачивания ПО «Jinn-Client»

7) в окне «Настройка параметров «Jinn-Client»» нажмите кнопку «Далее» (Рисунок 23);

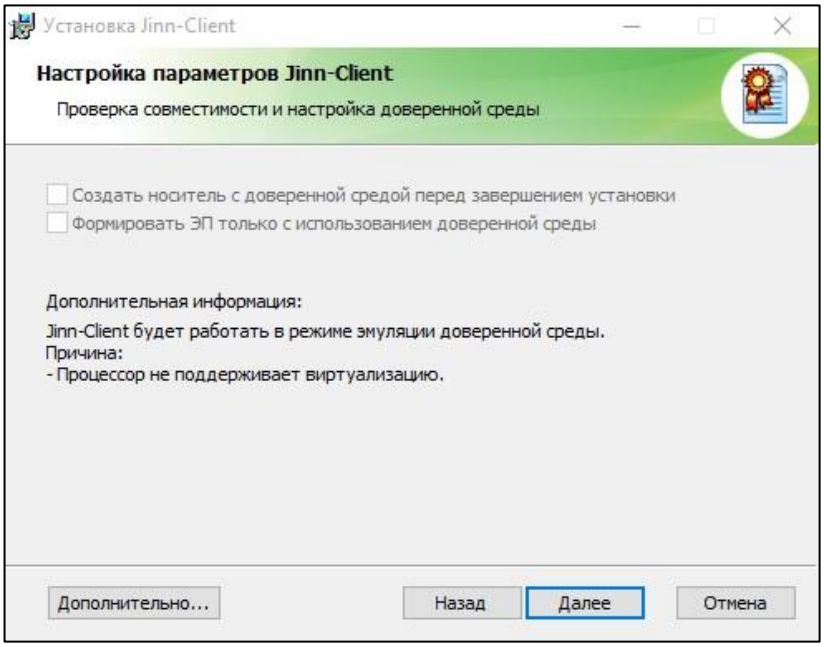

Рисунок 23 – Окно «Настройка параметров «Jinn-Client»»

8) в окне «Все готово к установке» нажмите кнопку «Установить», запустится процесс установки «Jinn-Client» (Рисунок 24);

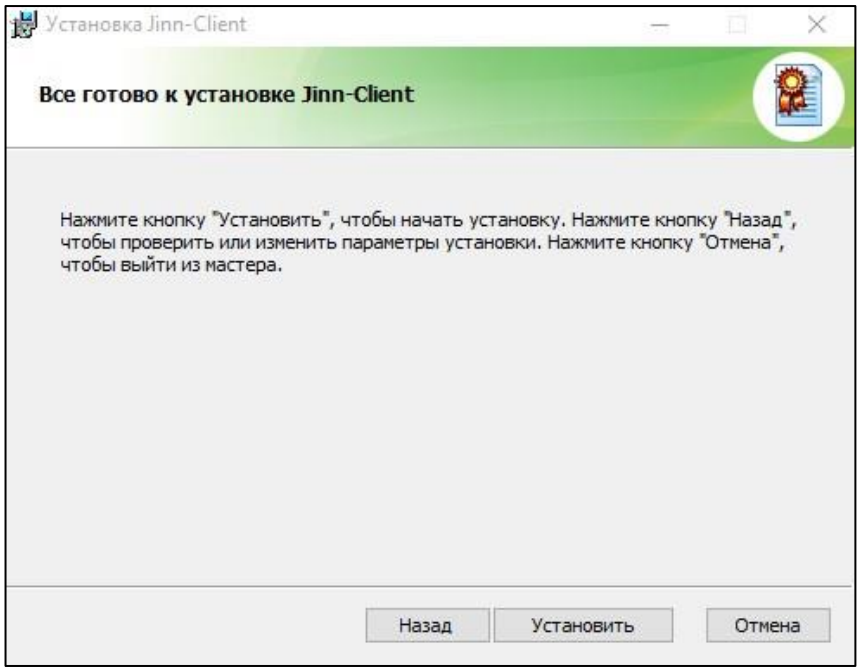

Рисунок 24 – Окно «Все готово к установке»

9) в окне «Установка Jinn-Client завершена» нажмите кнопку «Готово» (Рисунок 25);

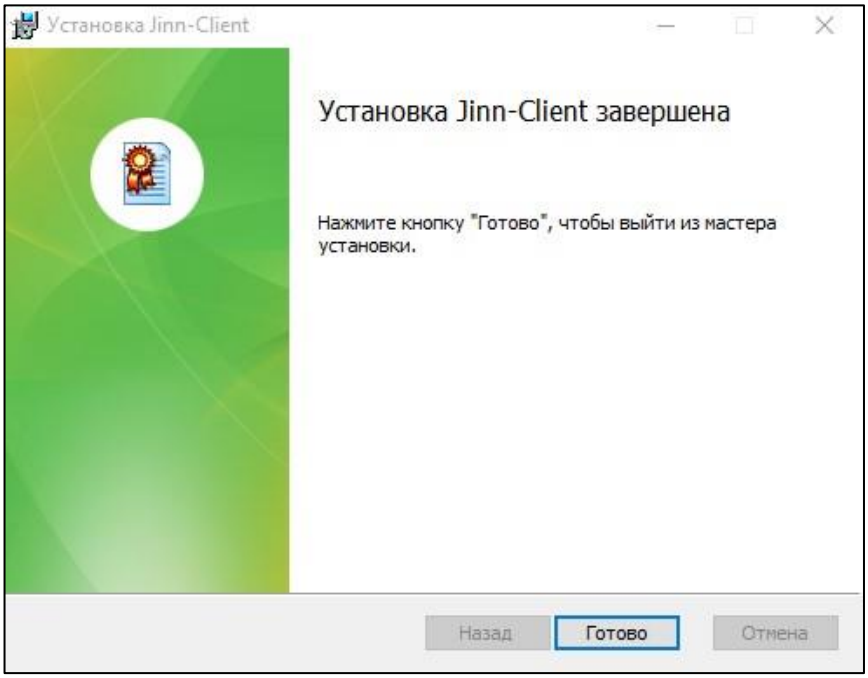

Рисунок 25 – Окно «Установка Jinn-Client завершена»

10) на экране появится сообщение с предложением перезагрузить компьютер. Если установка других компонентов не требуется, выберите кнопку «Да», начнется перезагрузка компьютера (Рисунок 26).

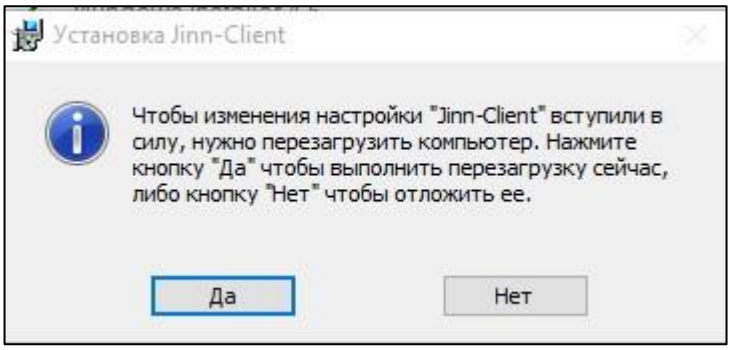

Рисунок 26 – Предложение перезагрузить компьютер

Для установки и настройки ПО «Jinn Sign Extension» в web-браузере, например «Google Chrome», выполните следующую последовательность действий:

1) откройте web-браузер, нажмите кнопку вызова меню настроек и управления web-браузером. Выберете пункт «Дополнительные инструменты», затем пункт «Расширения» (Рисунок 27);

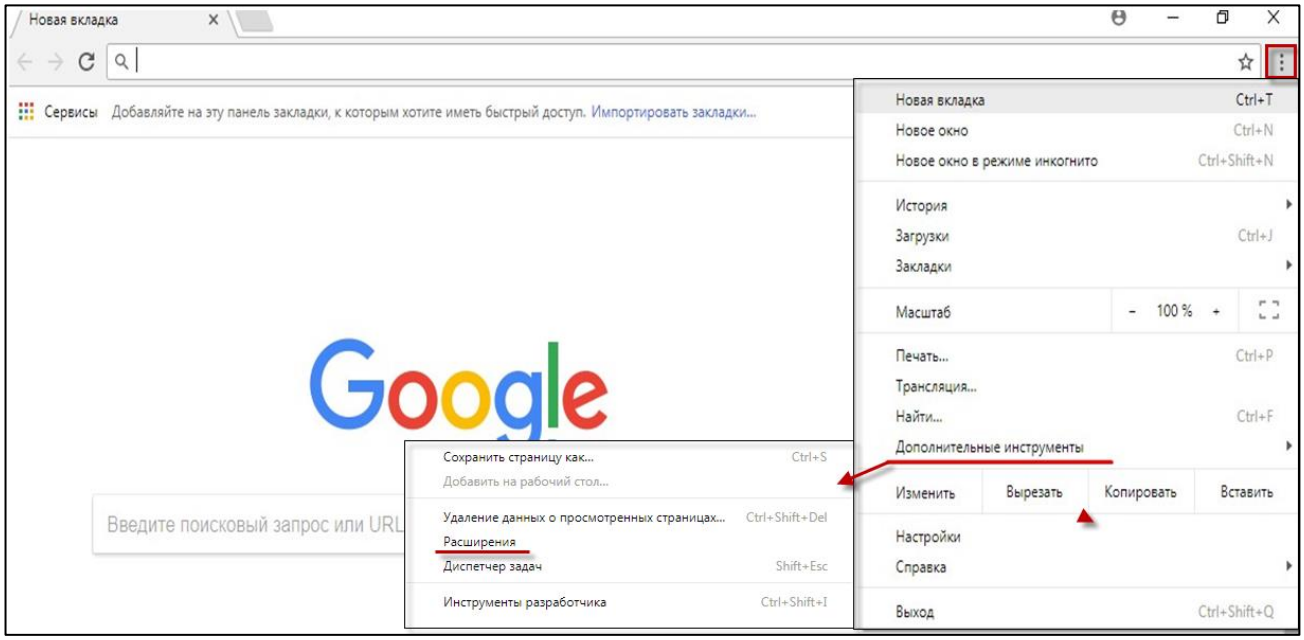

Рисунок 27 – Пункт «Дополнительные инструменты/Расширения»

2) в окне «Расширения» выберите пункт «Еще расширения» (Рисунок 28);

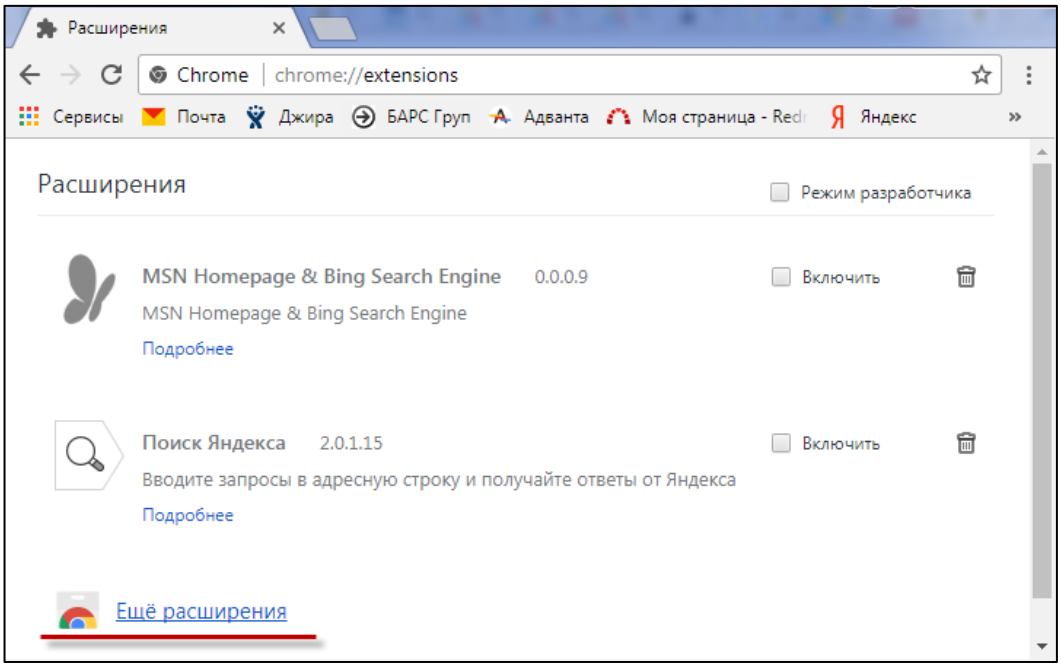

Рисунок 28 – Пункт «Еще расширения»

3) отобразится окно «Интернет-магазин Chrome». В строку поиска введите значение «jinn», в предложенном списке значений выберите «jinn sign extension». Убедитесь, что программный продукт, который вы хотите установить, с ресурса www.securitycode.ru – должна быть надпись «предлагается на сайте www.securitycode.ru» (Рисунок 29);

Рисунок 29 – ПО «Jinn Sign Extension» с ресурса www.securitycode.ru

4) нажмите кнопку «Установить»;
5) отобразится окно «Установить «Jinn Sign Extension»?», нажмите кнопку «Установить расширение» (Рисунок 30);

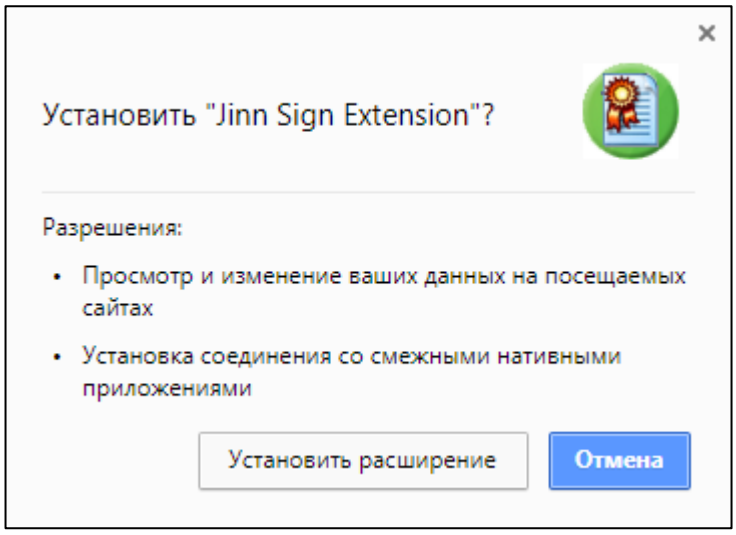

Рисунок 30 – Окно «Установить «Jinn sign Extension»?»

6) после установки расширения вернитесь в раздел «Расширения», отыщите информацию о «Jinn Sign Extension» и установите «флажок» по параметру «Разрешить открывать локальные файлы по ссылкам» (Рисунок 31).

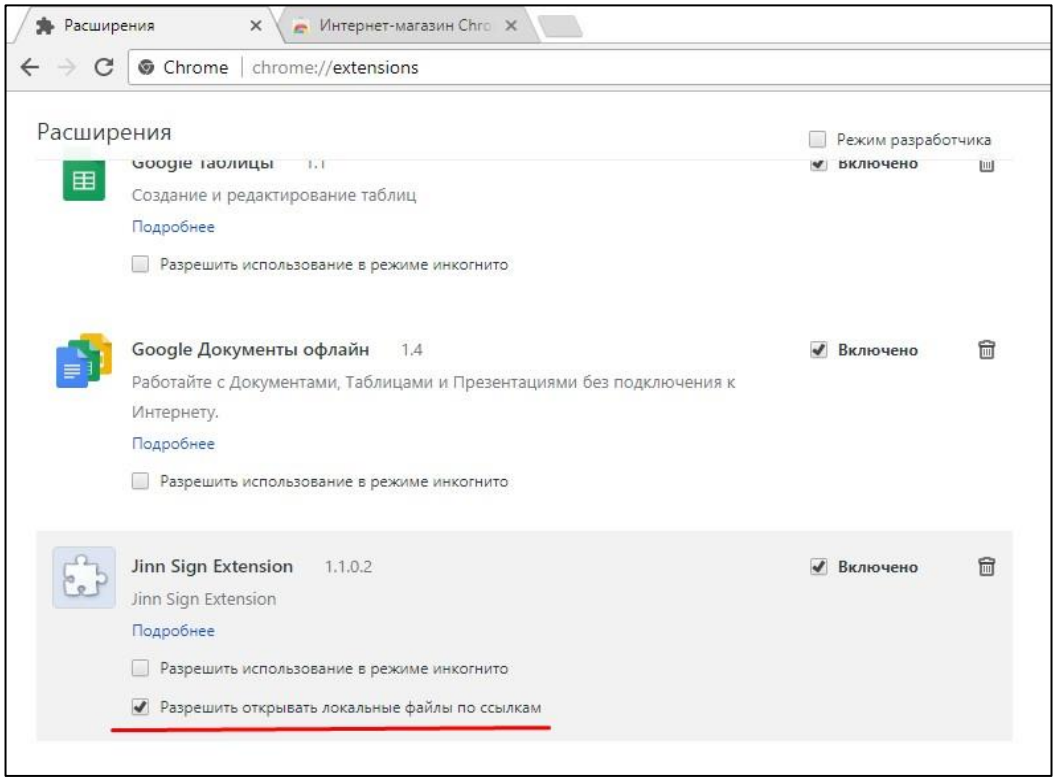

Рисунок 31 – Назначение параметра «Разрешить открывать локальные фалы по ссылкам»

Установка и настройка ПО «Jinn Sign Extension» завершена.

6.1 Установка ПО и расширения Jinn Sign Extension

После установки ПО «Jinn-Client» требуется установка ПО и расширения JinnSignExtension. Откройте папку, в которой находился установочный файл ПО «Jinn-Client». Найдите папку «prerequisites» (Рисунок 32).

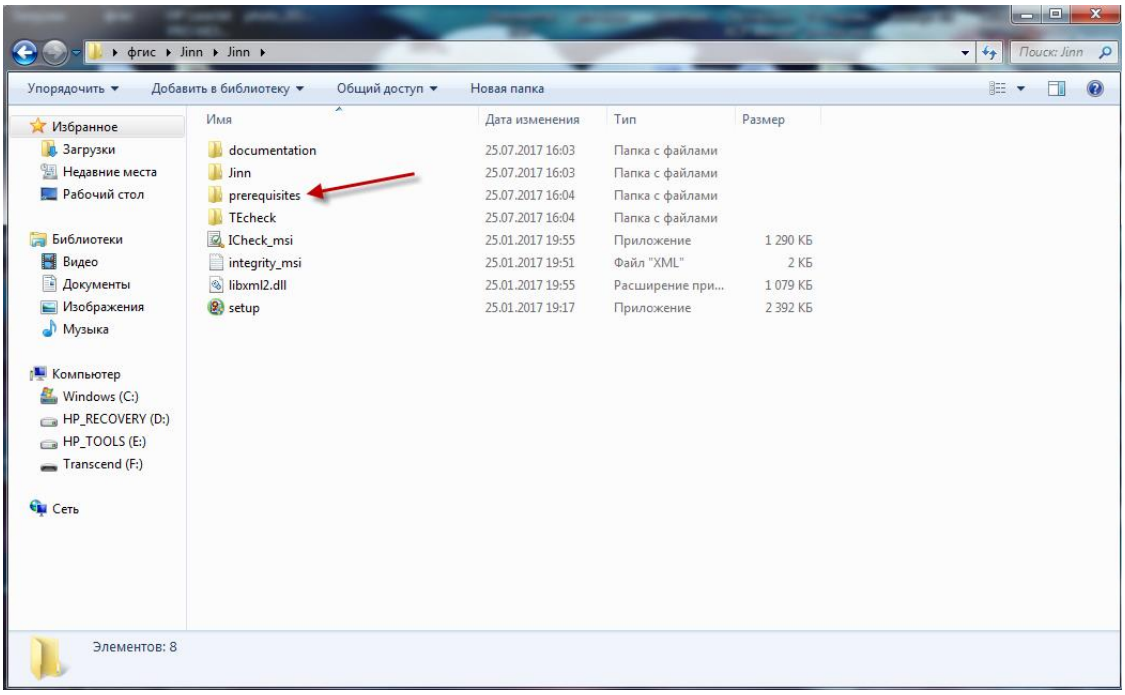

Рисунок 32 – Папка с установочным файлом ПО JinnSignExtension

Запустите установочный файл «JinnSignExtensionSetup» от имени администратора.

Для установки программы откроется окно мастера установки Jinn Sign Extension Provider. В открывшемся окне нажмите кнопку «Далее» (Рисунок 33).

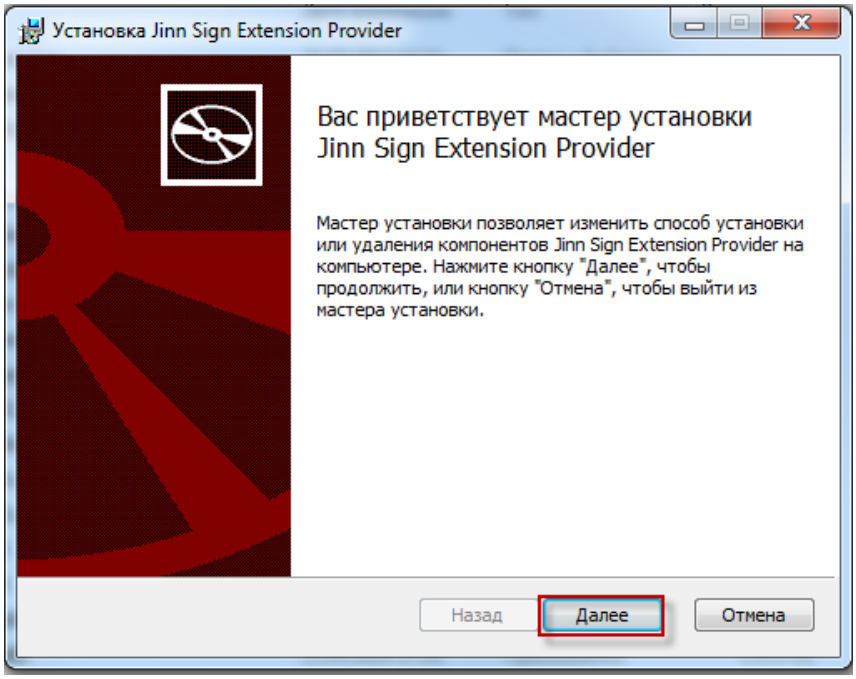

Рисунок 33 – Стартовое окно мастера установки

Следующим шагом установите «флажок» в поле «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее» (Рисунок 34).

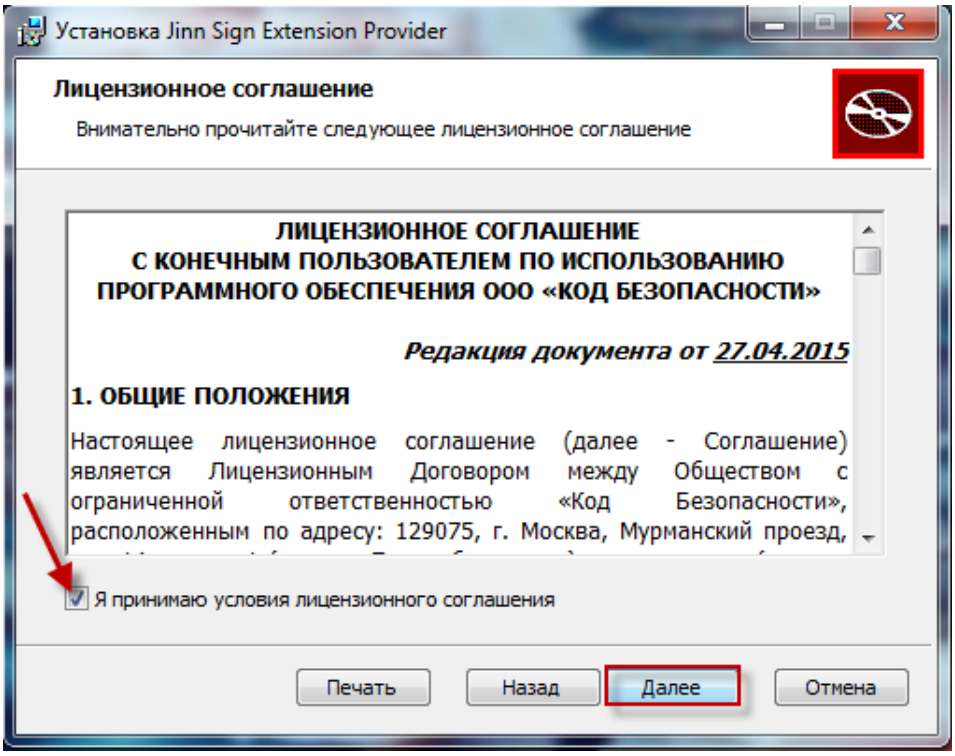

Рисунок 34 – Лицензионное соглашение

В следующем окне измените путь для установки ПО JinnSignExtension на «C:\Program Files\Securite Code». Для этого очистите строку, где прописан путь, до значения «C:\» и нажмите кнопку «Изменить»(Рисунок 35).

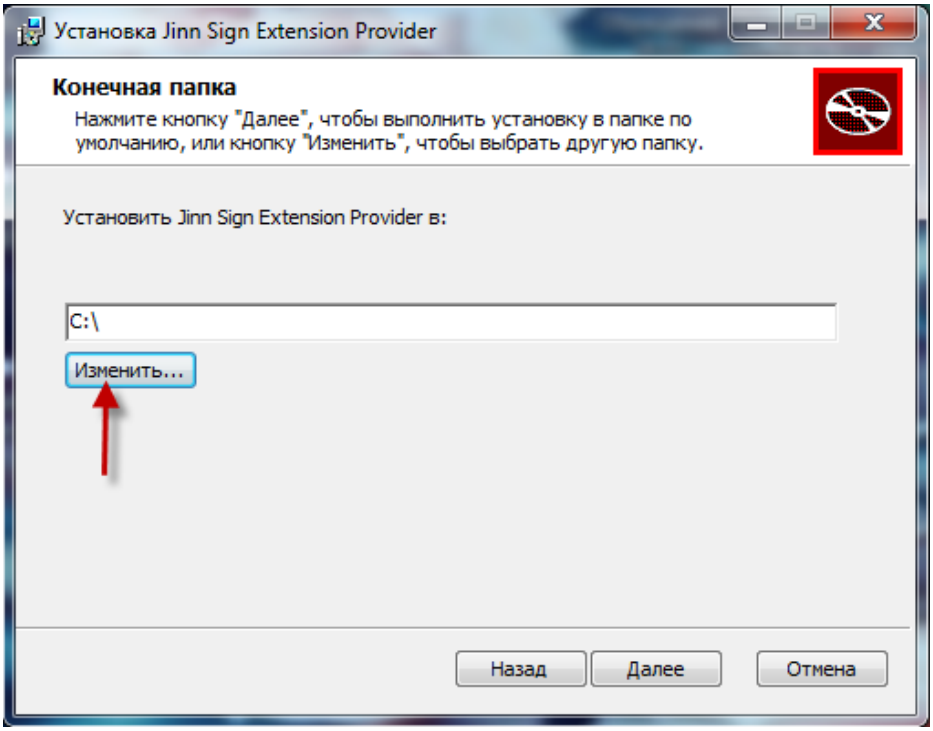

Рисунок 35 – Окно конечной папки для установки ПО JinnSignExtension

Выберите папку «Program Files» (Рисунок 36).

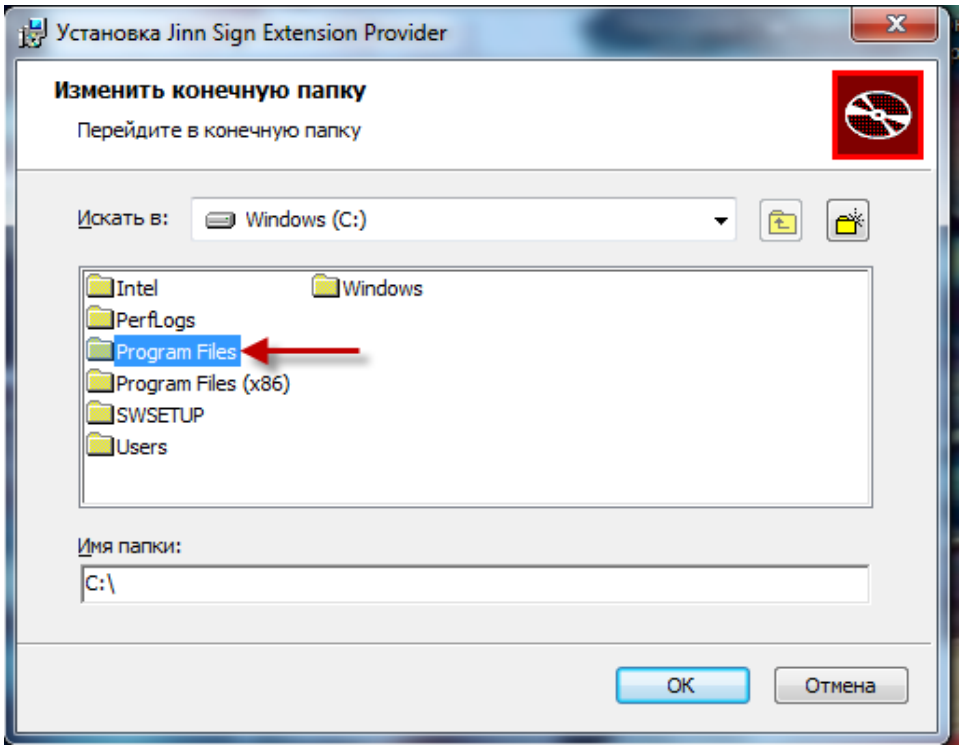

Рисунок 36 – Изменение конечной папки. Шаг 1

Далее найдите папку «Securite Code», выберите ее в качестве конечной папки и нажмите кнопку «Ок» (Рисунок 37).

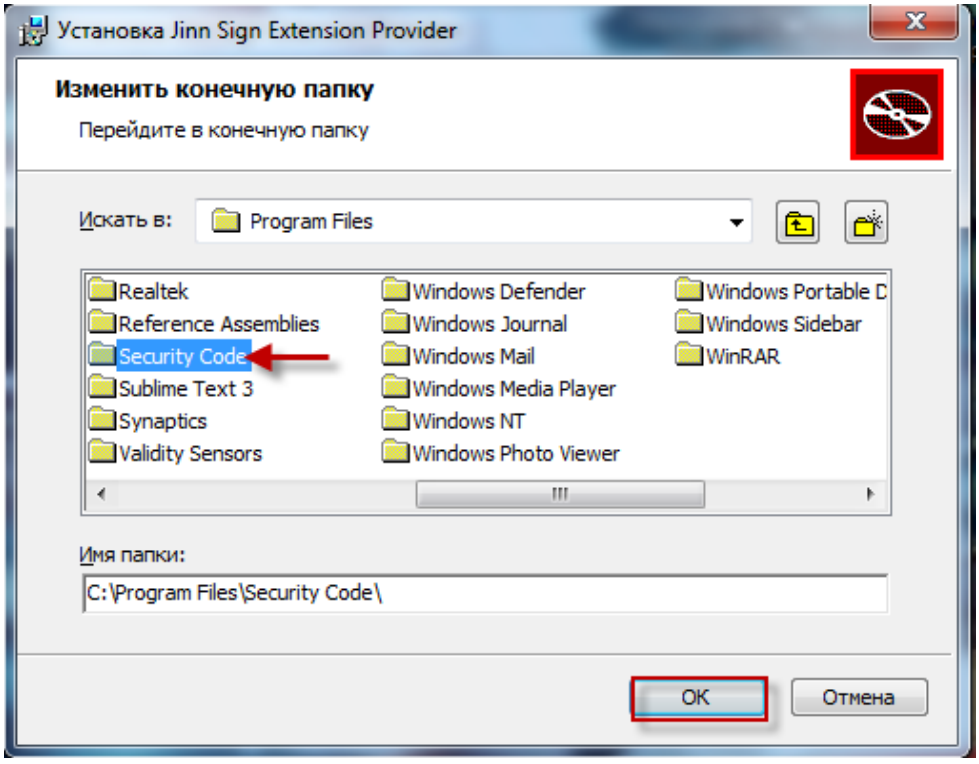

Рисунок 37 – Изменение конечной папки. Шаг 2

Нажмите кнопку «Далее» (Рисунок 38).

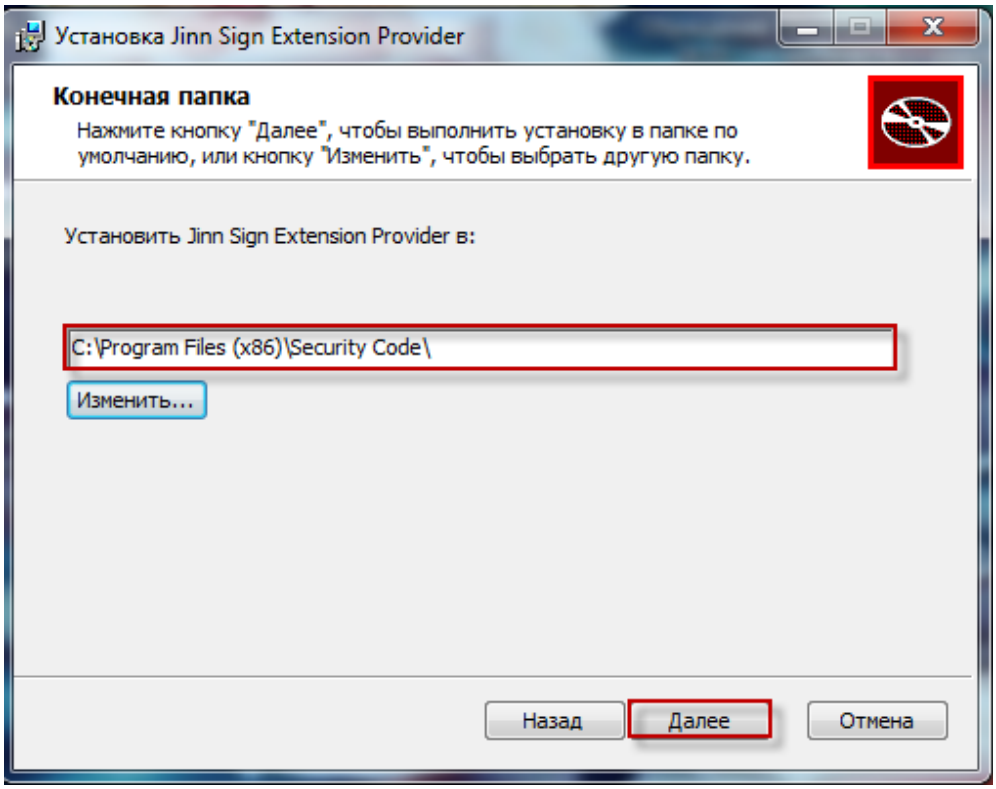

Рисунок 38 – Изменение конечной папки. Шаг 3

В следующем окне нажмите кнопку «Установить» (Рисунок 39).

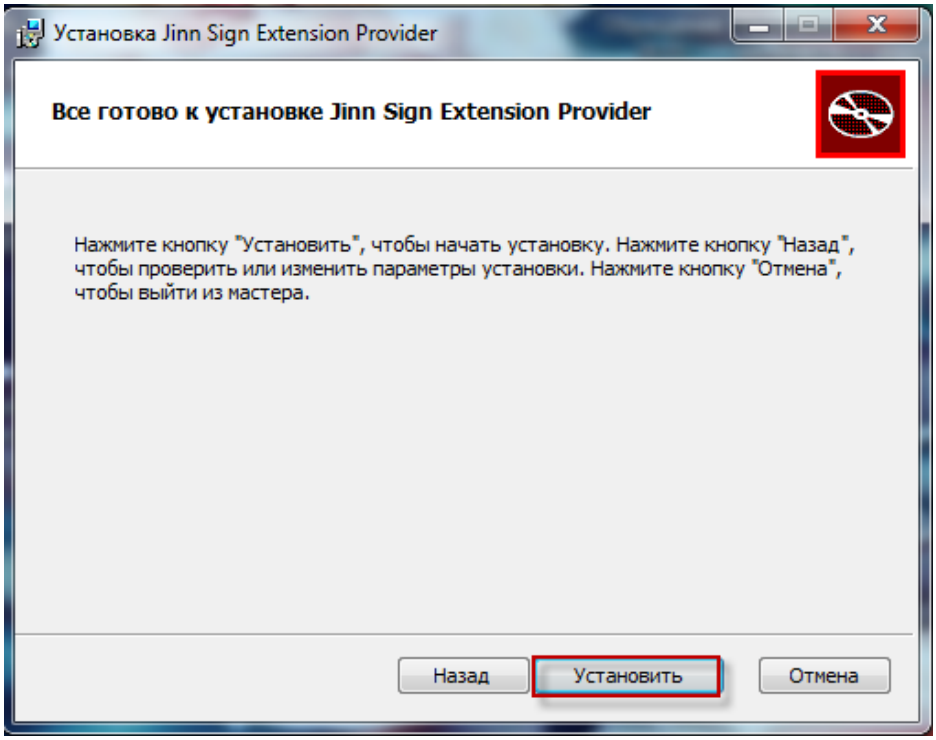

Рисунок 39 – Установка ПО JinnSignExtension

По завершении установки откроется диалоговое окно с сообщением об успешном завершении установки. Нажмите кнопку «Готово» (Рисунок 40).

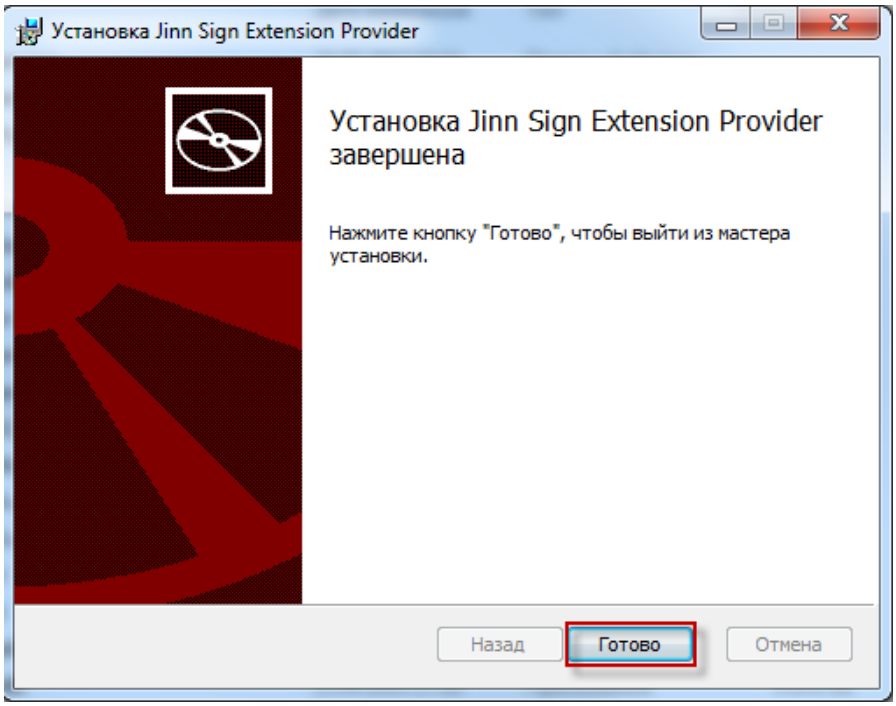

Рисунок 40 – Сообщение об успешном завершении установки ПО JinnSignExtension

Следующим шагом установите расширение Jinn Sign Extension для браузера. Для этого запустите браузер, в меню браузера выберите пункт «Дополнительные инструменты/ Расширения» (Рисунок 41).

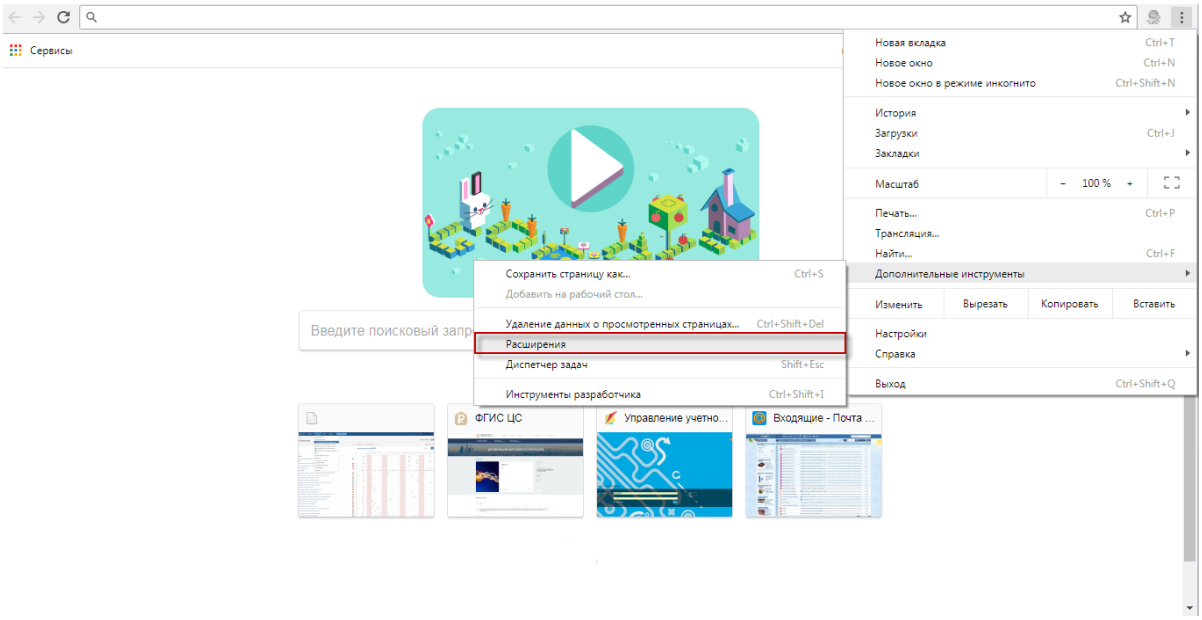

Рисунок 41 – Установка расширения Jinn Sign Extension для браузера. Шаг 1

В открывшемся окне найдите пункт «Еще расширения» и нажмите на него (Рисунок 42).

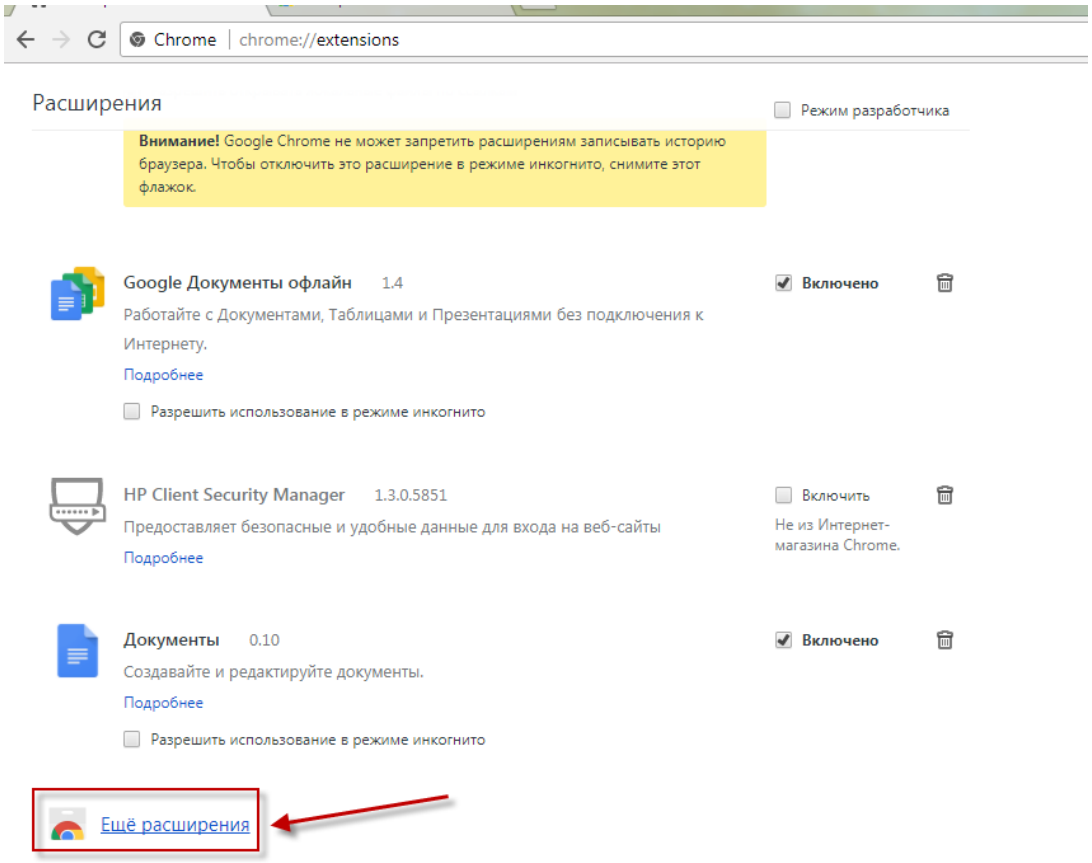

Рисунок 42 – Установка расширения Jinn Sign Extension для браузера. Шаг 2

Откроется окно интернет магазина, в строке поиска введите «jinn» (Рисунок 43).

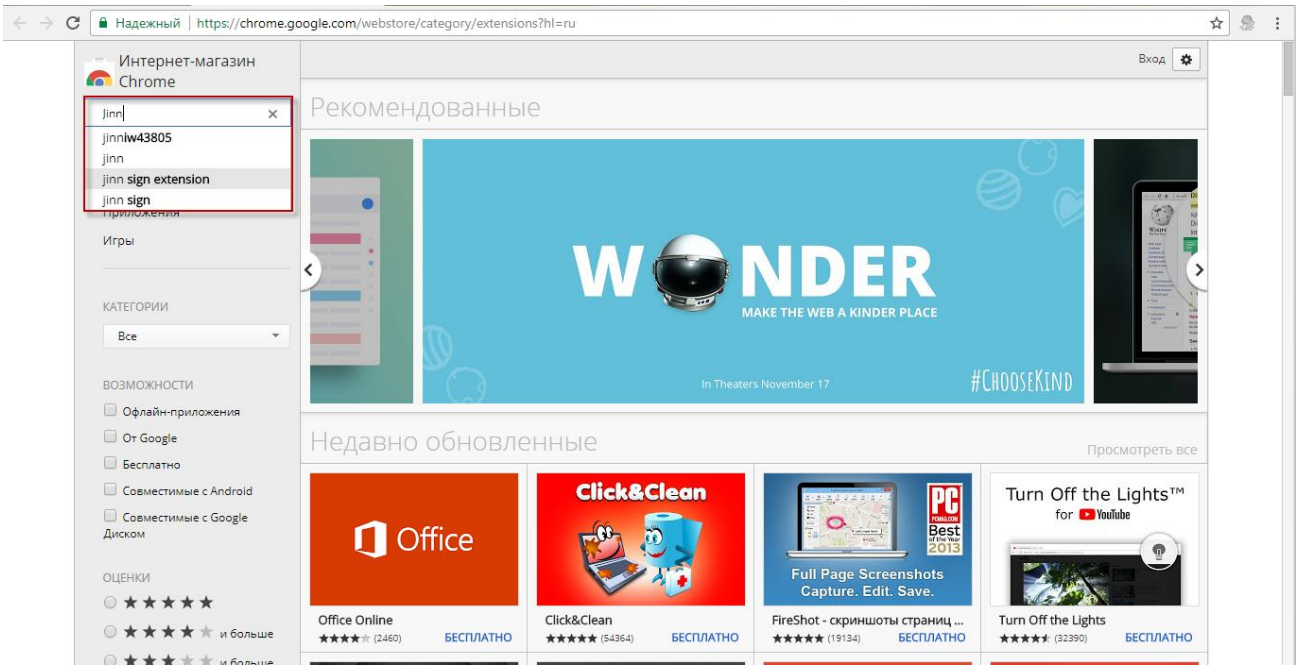

Рисунок 43 – Установка расширения Jinn Sign Extension для браузера Шаг 3

Выберите из списка Jinn Sign Extension и нажмите кнопку «Установить» (Рисунок 44).

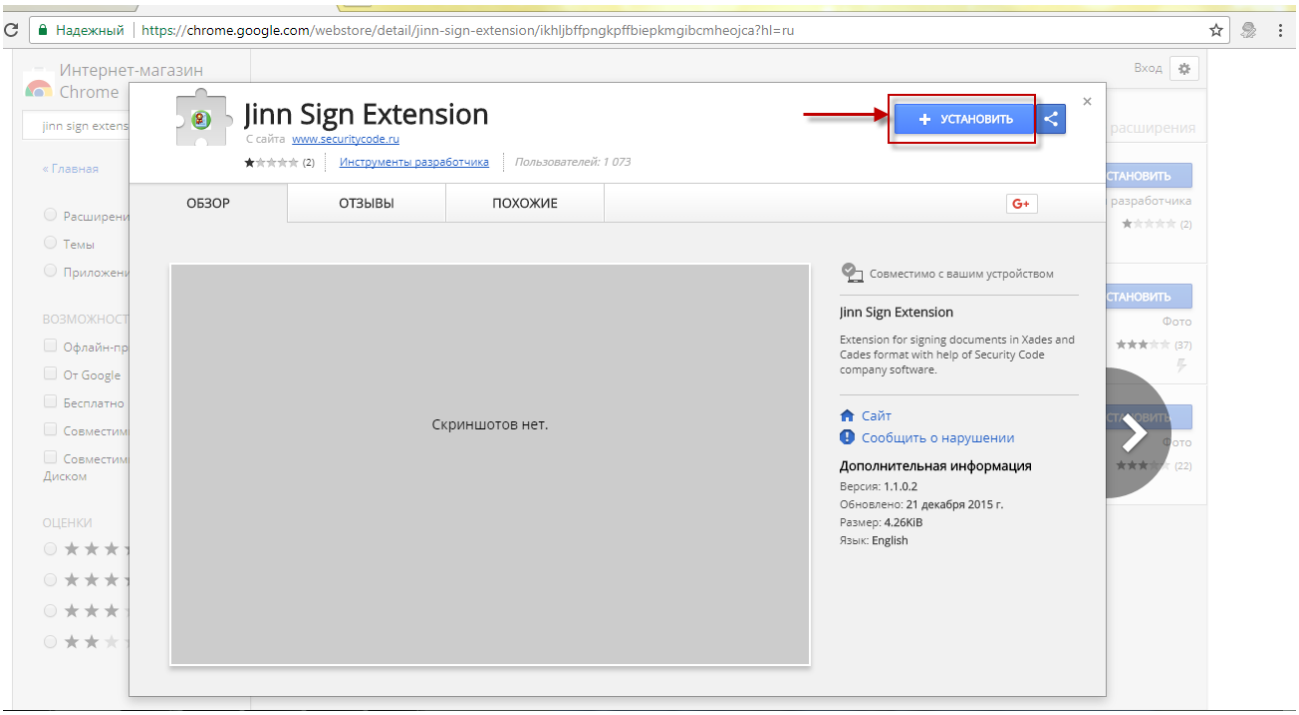

Рисунок 44 – Установка расширения Jinn Sign Extension для браузера. Шаг 4

Во всплывающем окне нажмите кнопку «Установить расширение» (Рисунок 45).

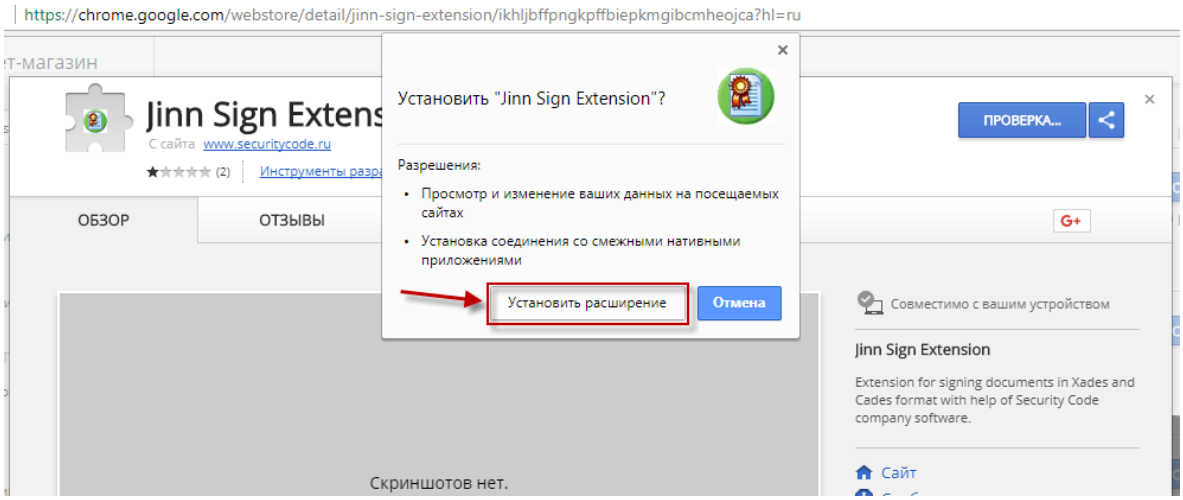

Рисунок 45 – Установка расширения Jinn Sign Extension для браузера. Шаг 5

По завершении установки расширения откроется всплывающее окно с сообщением об успешной установке расширения Jinn Sign Extension (Рисунок 46).

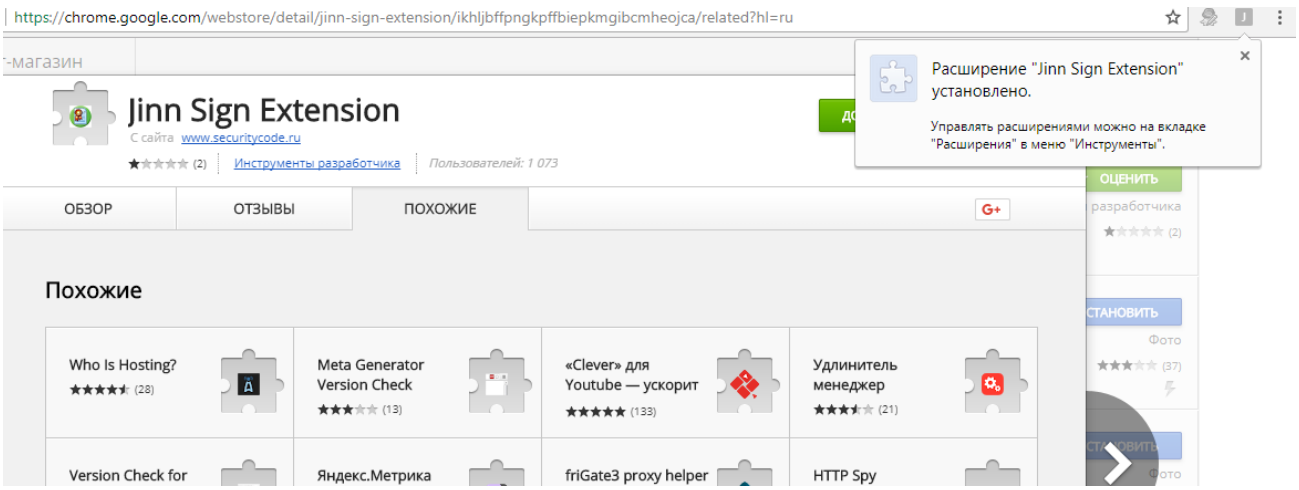

Рисунок 46 – Установка расширения Jinn Sign Extension для браузера. Шаг 6

Затем повторно откройте панель инструментов и перейдите в раздел «Расширения».

Убедитесь, что у расширения Jinn Sign Extension установлен «флажок» в поле «включено» (Рисунок 47). При необходимости установите «флажки» в полях «Разрешить использование в режиме инкогнито» и «Разрешить открывать локальные файлы по ссылкам». Установка расширения Jinn Sign Extension завершена.

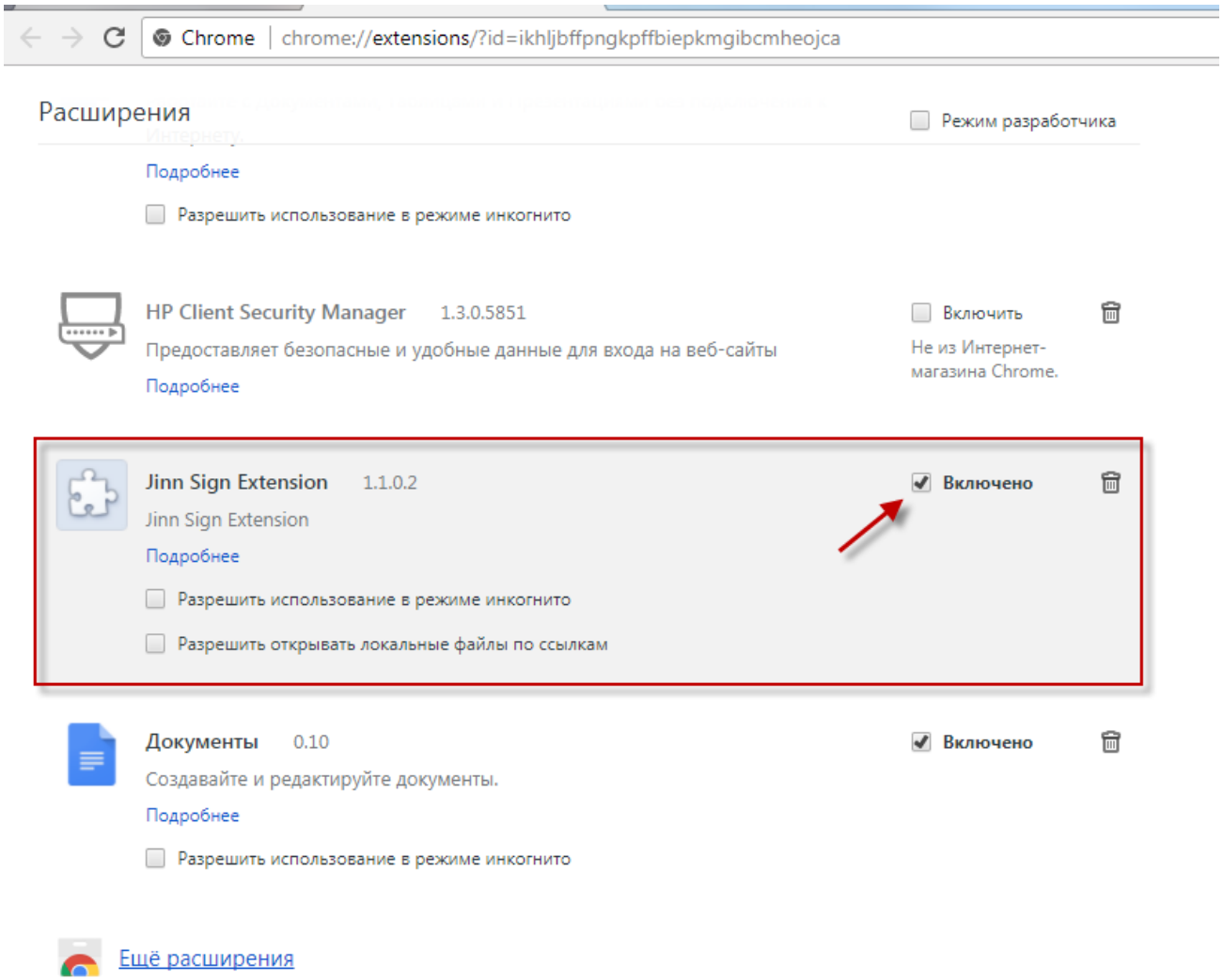

Рисунок 47 – Проверка установки расширения

7 Установка ПО «Континент TLS VPN»

Для корректной работы с ФГИС ЦС установите ПО «Континент TLS VPN», предназначенное для обеспечения защищенного доступа удаленных пользователей к ФГИС ЦС по каналам связи общих сетей передачи данных.

Откройте каталог с ПО «Континент TLS VPN».

До начала установки ПО «Континент TLS VPN» заполните заявку на получение лицензии. Лицензию получают в соответствии с общим порядком, установленным конкретным Удостоверяющим центром. Также после установки ПО «Континент TLS VPN» заполните акт установки.

Обратите внимание, что перед установкой ПО «Континент TLS VPN» корневой сертификат уже должен быть установлен в нужный каталог (см. п. 5).

Далее приступите к установке ПО «Континент TLS VPN»:

1) поместите установочный диск в устройство чтения компакт-дисков и запустите к исполнению файл «ContinentTLSSetup.exe» (Рисунок 48);

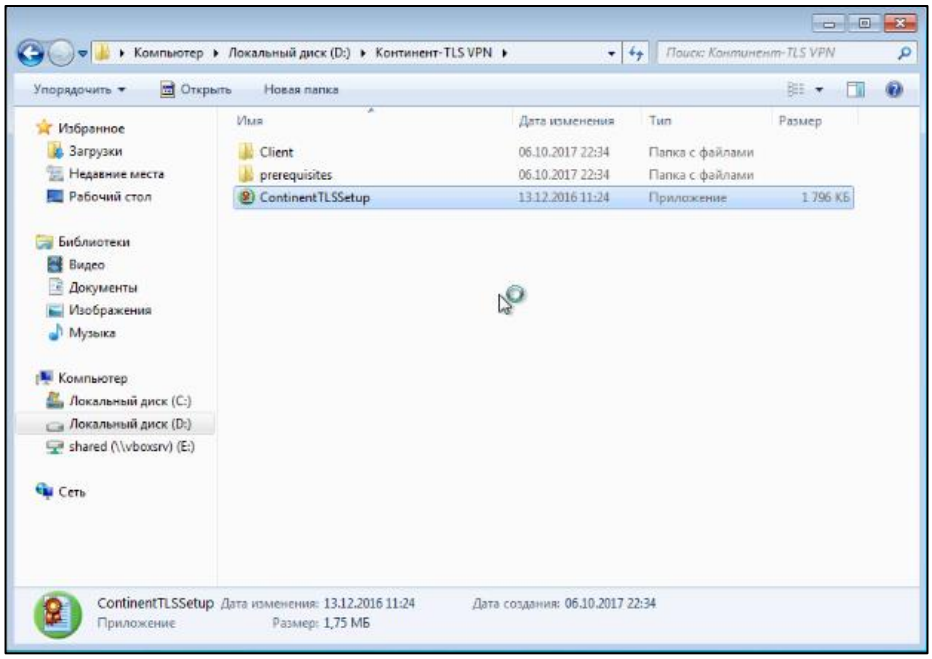

Рисунок 48 – Установочный файл «ContinentTLSSetup.exe»

Из всех перечисленных компонентов обязательным для установки является «Континент TLS Клиент в исполнении КС1» (Рисунок 49).

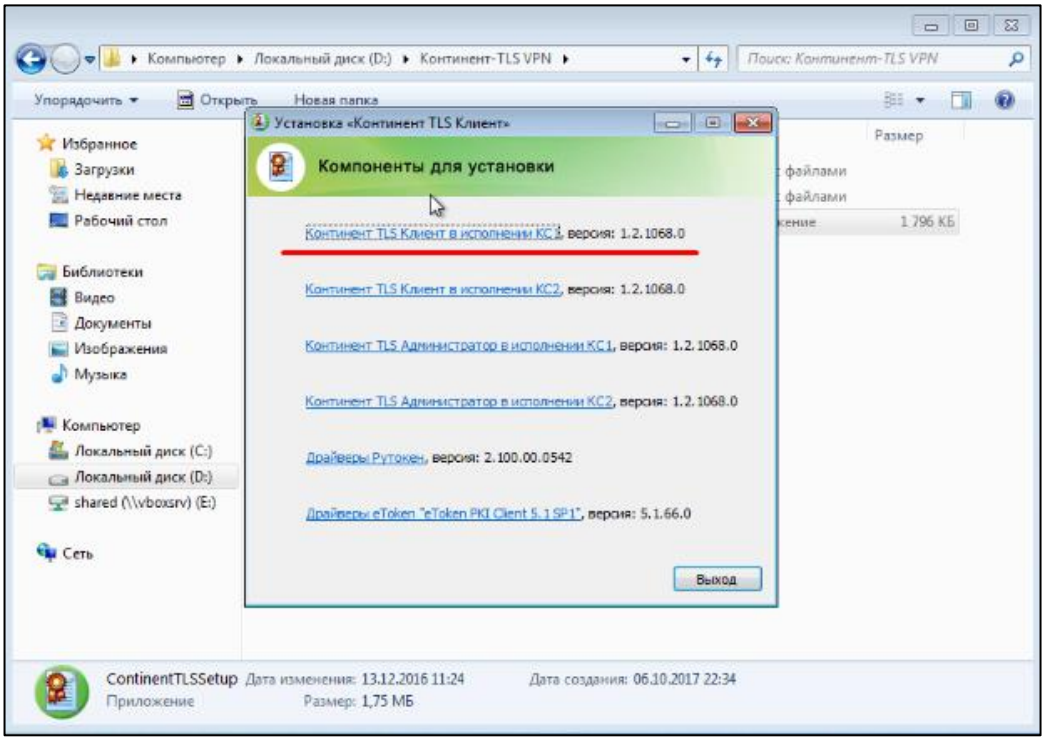

Рисунок 49 – Компонент «Континент TLS Клиент в исполнении КС1»

2) выберите компонент «Континент TLS Клиент в исполнении КС1». На экране появится стартовое окно мастера установки компонента (Рисунок 50). Нажмите кнопку «Далее»;

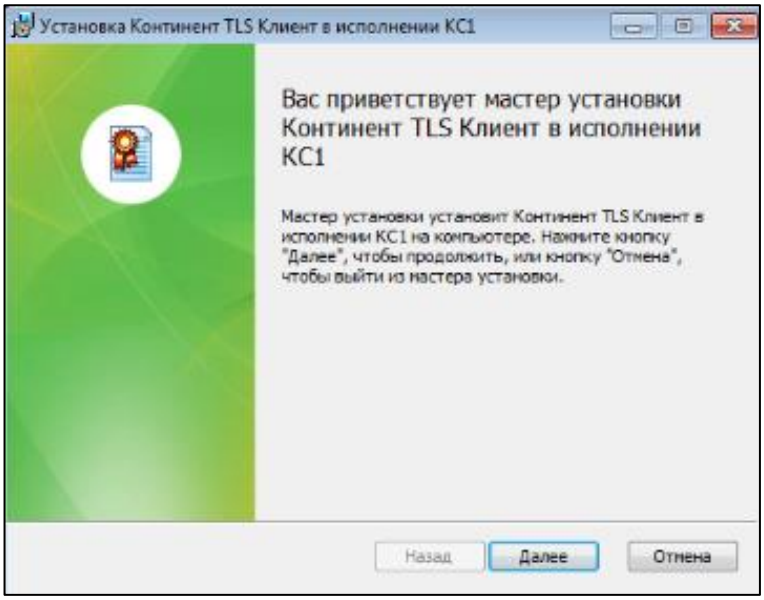

Рисунок 50 – Окно мастера установки компонента «Континент TLS Клиент в исполнении КС1»

3) на экране появится окно лицензионного соглашения. Согласитесь с условиями лицензионного соглашения, установив «флажок» по параметру «Я принимаю условия» и нажав кнопку «Далее» (Рисунок 51);

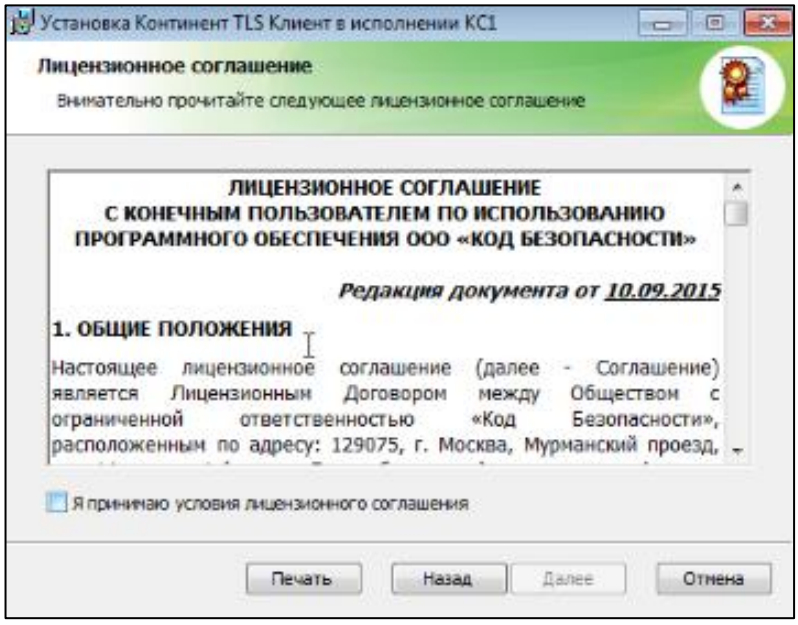

Рисунок 51 – Окно лицензионного соглашения

4) отобразится окно выбора каталога локального компьютера для разворачивания в нем компонента «Континент TLS Клиент в исполнении КС1». По умолчанию разворачивание выполнится на системный диск в каталог: **\Program Files\SecurityCode\Континент TLS Клиент_КС1**. Чтобы выбрать другой каталог, нажмите кнопку «Изменить» и задайте нужную директорию, затем нажмите кнопку «Далее» (Рисунок 52);

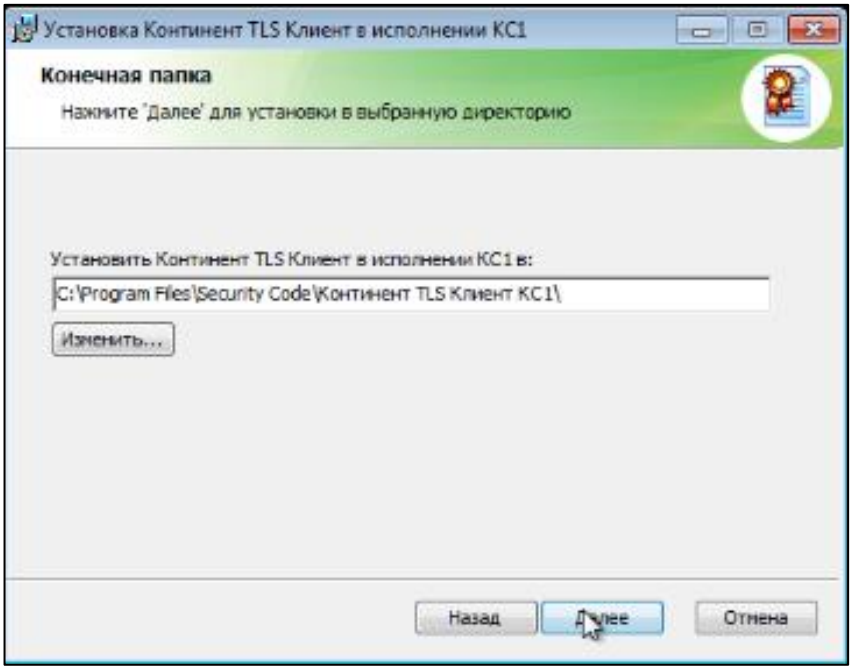

Рисунок 52 – Расположение каталога для разворачивания компонента «Континент TLS Клиент в исполнении КС1»

5) в окне с информацией о готовности к установке нажмите кнопку «Установить» (Рисунок 53). Запустится процесс установки, который продлится некоторое время;

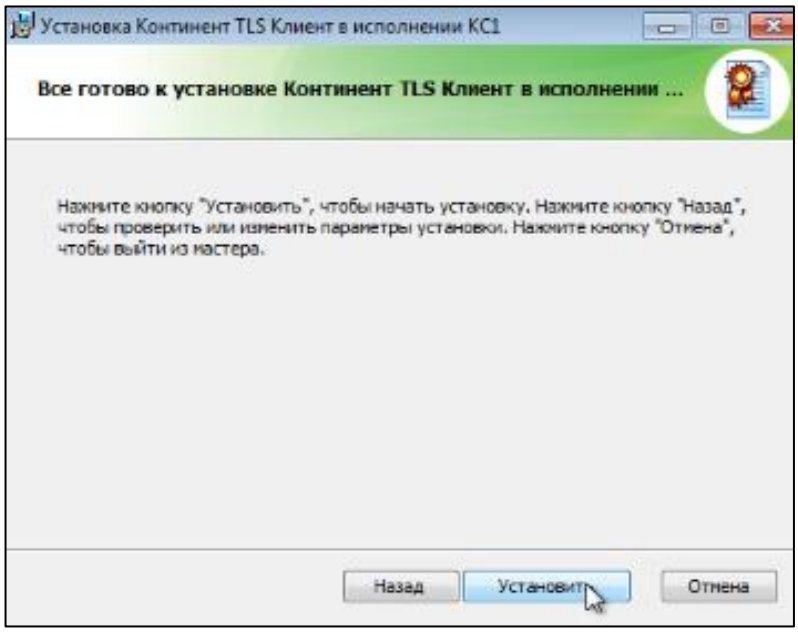

Рисунок 53 – Информация о готовности к установке компонента «Континент TLS Клиент в исполнении КС1»

6) в окне с информацией о завершении установки нажмите кнопку «Готово» (Рисунок 54).

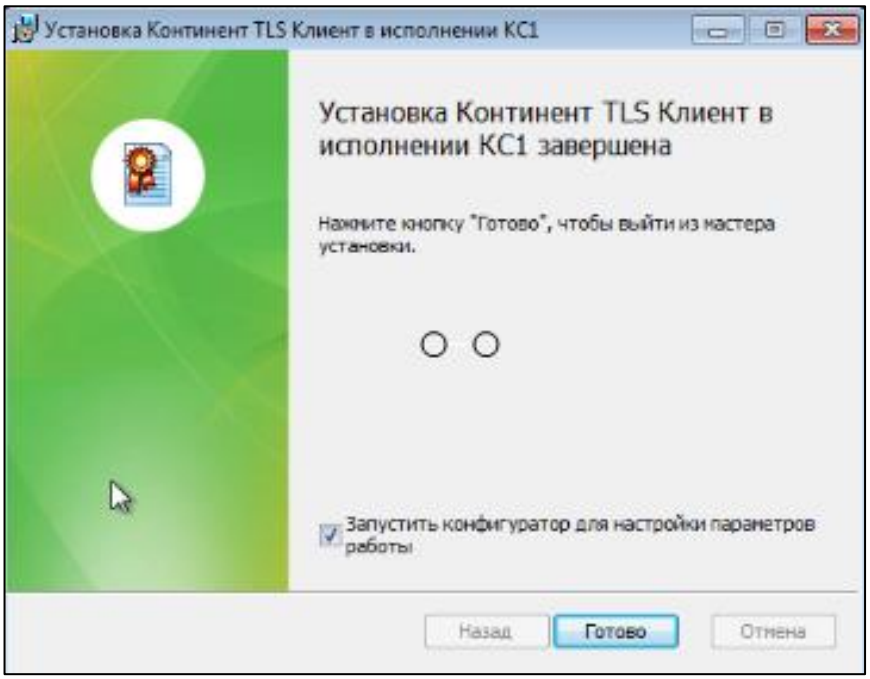

Рисунок 54 – Информация о завершении установки

7) отобразится окно «Код Безопасности CSP». Нацельтесь на появившееся изображение мишени и нажмите на него левой кнопкой мыши (Рисунок 55);

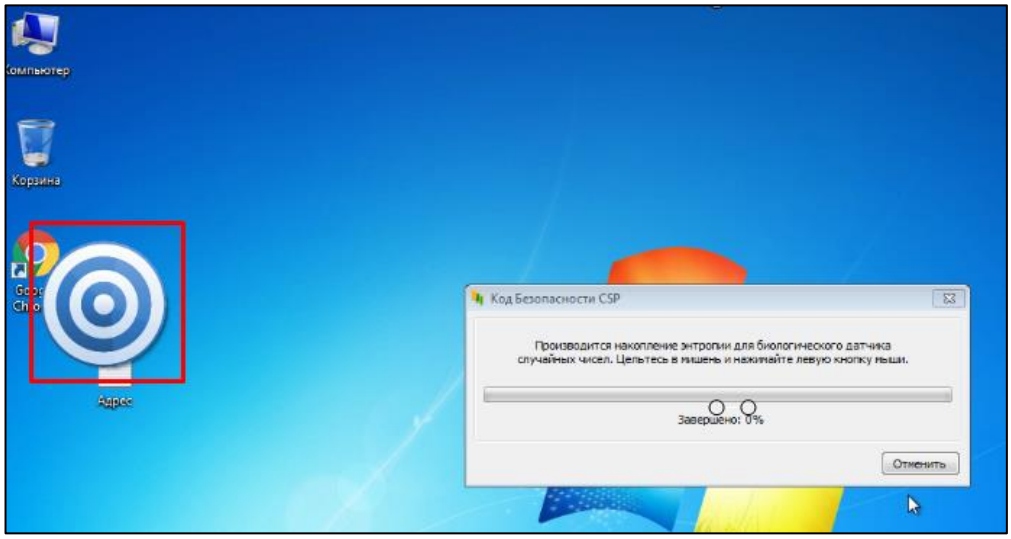

Рисунок 55 – Мишень

8) в окне «Вектор успешно изменен» нажмите кнопку «ОК»;

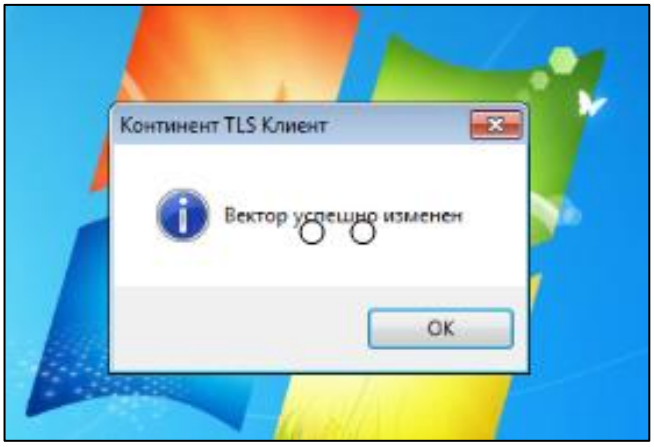

Рисунок 56 – Окно «Вектор успешно изменен»

9) в результате откроется окно «Настройки Континент TLS Клиента КС1». Перейдите на вкладку «Настройки программы» (Рисунок 57);

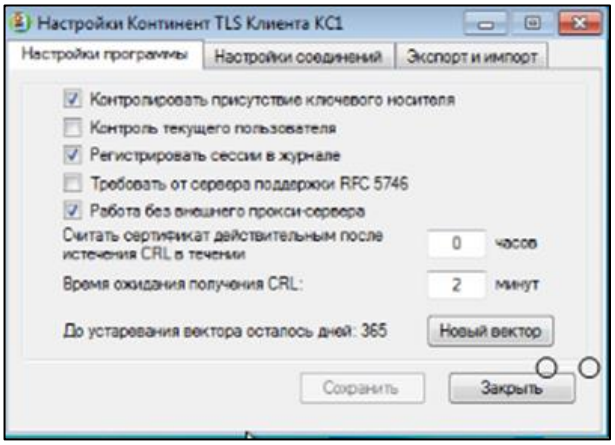

Рисунок 57 – Закладка «Настройки программы»

10) убедитесь, что установлены следующие разрешения:
    - «Контролировать присутствие ключевого носителя»;
    - «Регистрировать сессии в журнале»;
    - «Работа без внешнего прокси-сервера».
11) перейдите в закладку «Настройки соединений». Нажмите кнопку «Добавить соединение». В поле «Адрес/имя сервера» укажите значение «fgiscs-tls.gge.ru:8443», разрешите использовать туннель и нажмите кнопку «Далее» (Рисунок 58);

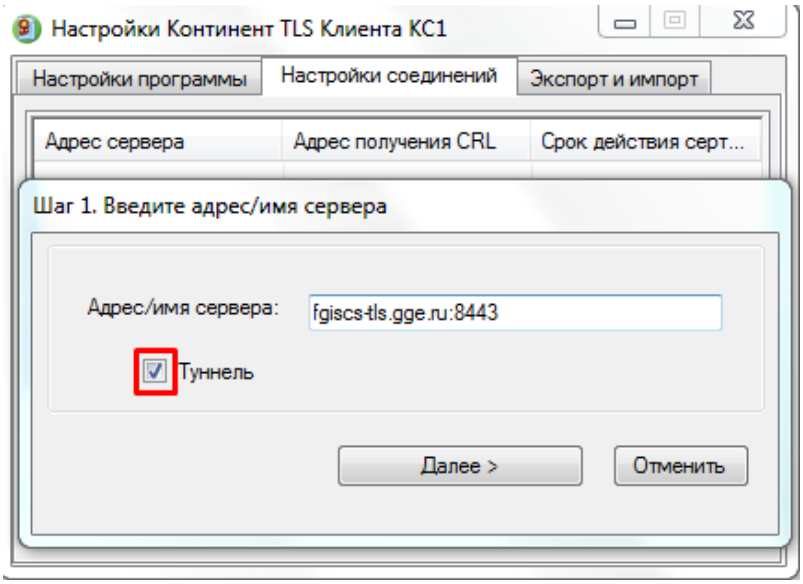

Рисунок 58 – Окно «Шаг 1. Введите адрес/имя сервера»

12) в окне «Шаг 2. Укажите сертификат сервера» нажмите кнопку «Выбрать сертификат» (Рисунок 59);

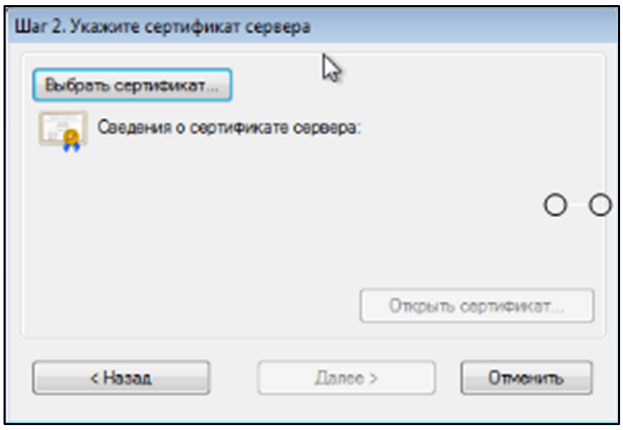

Рисунок 59 – Окно «Шаг 2. Укажите сертификат сервера»

13) укажите сертификат сервера (файл **fgiscs-tls.gge.ru (1).cer**), ранее полученный на Портале ФГИС ЦС в разделе «База знаний» в подразделе «Обучающие материалы». Нажмите кнопку «Открыть» (Рисунок 60);

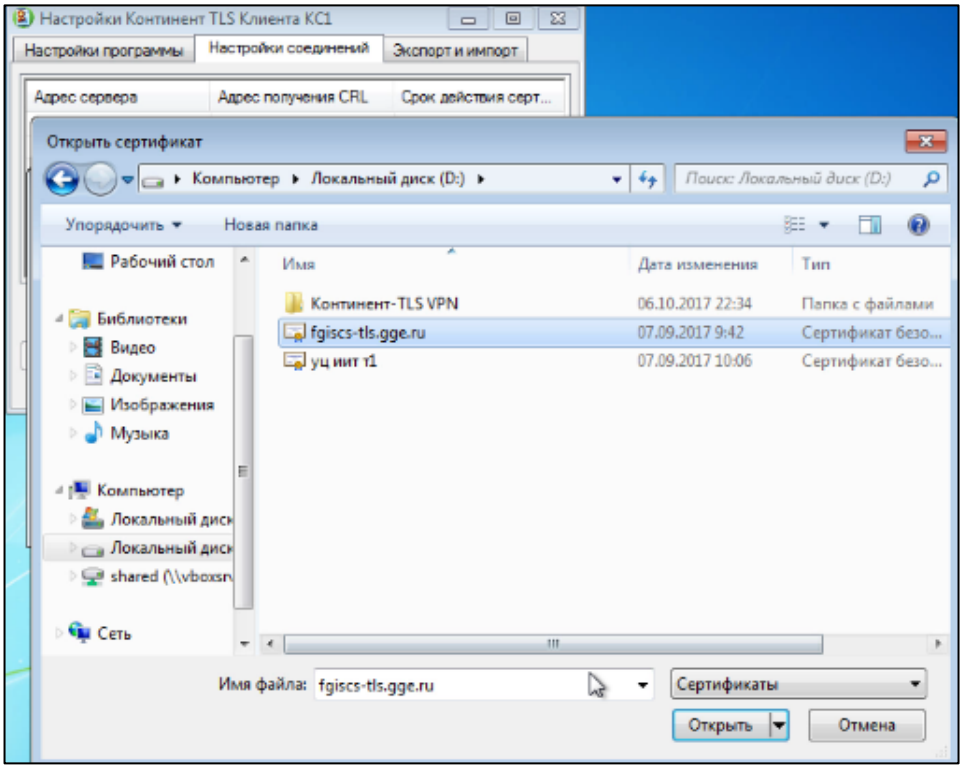

Рисунок 60 – Выбор сертификата

14) нажмите кнопку «Открыть сертификат» (Рисунок 61);

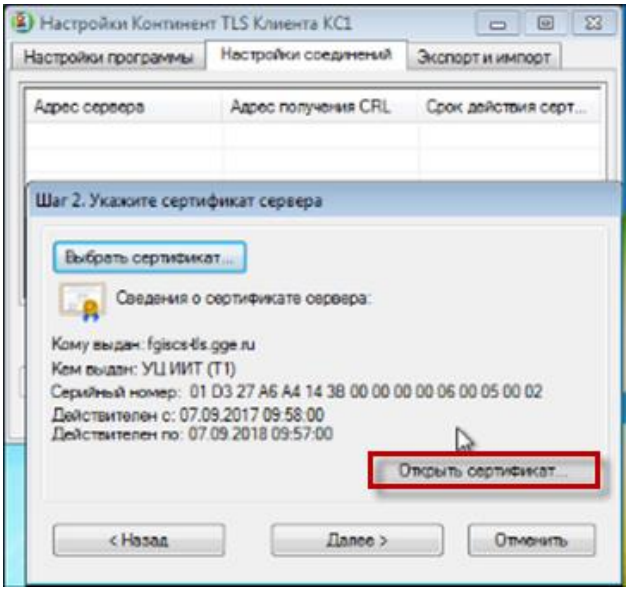

Рисунок 61 – Кнопка «Открыть сертификат»

15) в окне «Сертификат сервера» нажмите кнопку «Установить сертификат» (Рисунок 62);

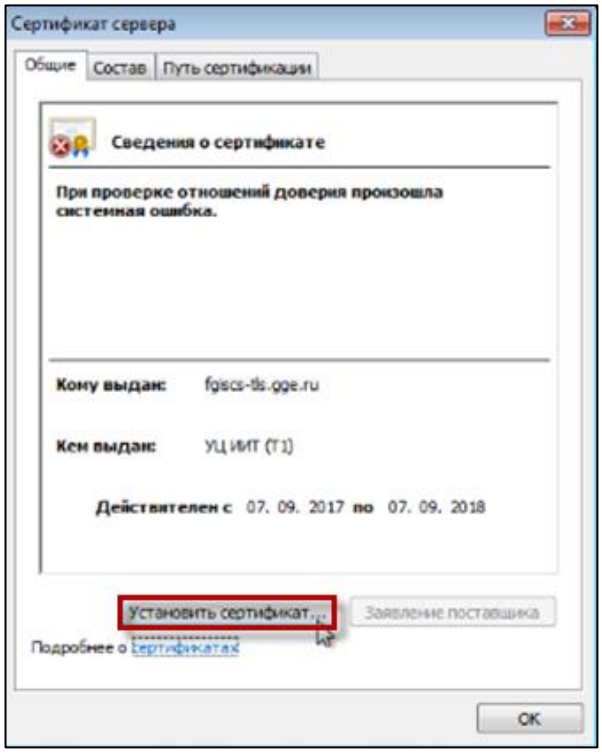

Рисунок 62 – Кнопка «Установить сертификат»

16) в окне «Мастер импорта сертификатов» нажмите кнопку «Далее» (Рисунок 63);

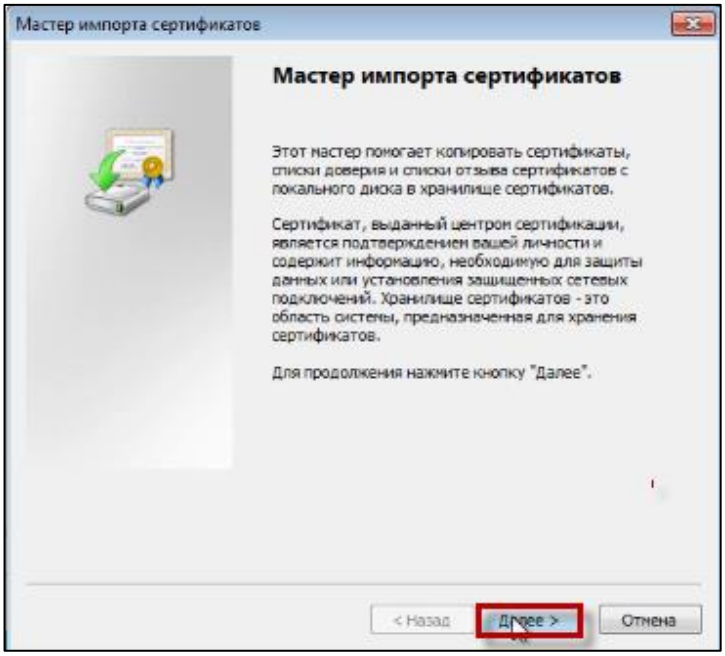

Рисунок 63 – Кнопка «Далее»

17) установите переключатель на параметр «Автоматически выбирать хранилище на основе типа сертификата», нажмите кнопку «Далее» (Рисунок 64);

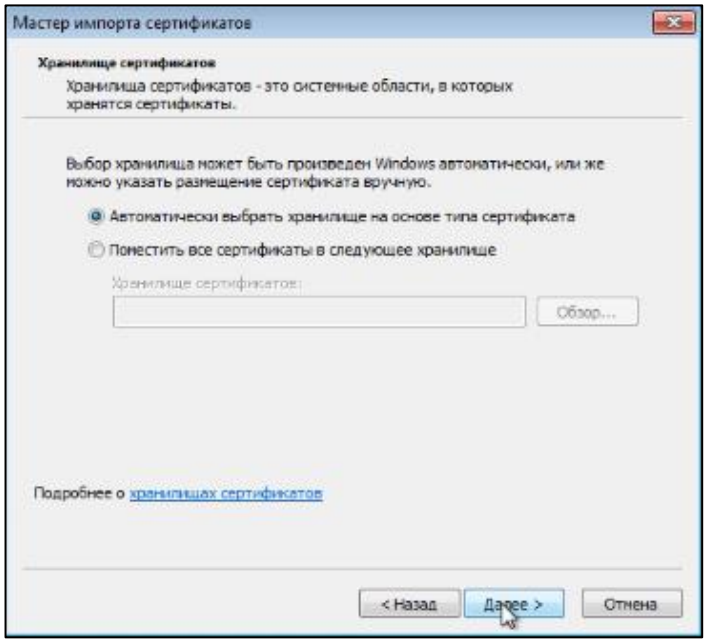

Рисунок 64 – Выбор параметра «Автоматически выбирать хранилище на основе типа сертификата»

18) в окне «Завершение мастера импорта сертификатов» нажмите кнопку «Готово» (Рисунок 65);

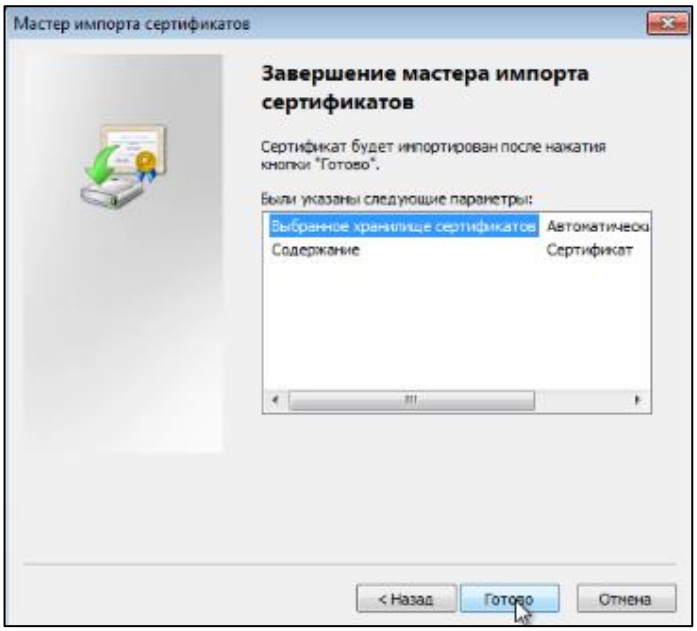

Рисунок 65 – Кнопка «Готово»

19) в окне «Импорт успешно выполнен» нажмите кнопку «ОК» (Рисунок 66);

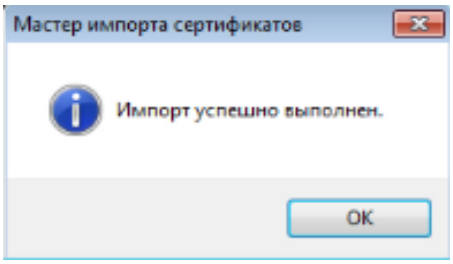

Рисунок 66 – Окно «Импорт успешно выполнен»

20) нажмите кнопку «ОК» для закрытия окна «Сертификат сервера» (Рисунок 67);

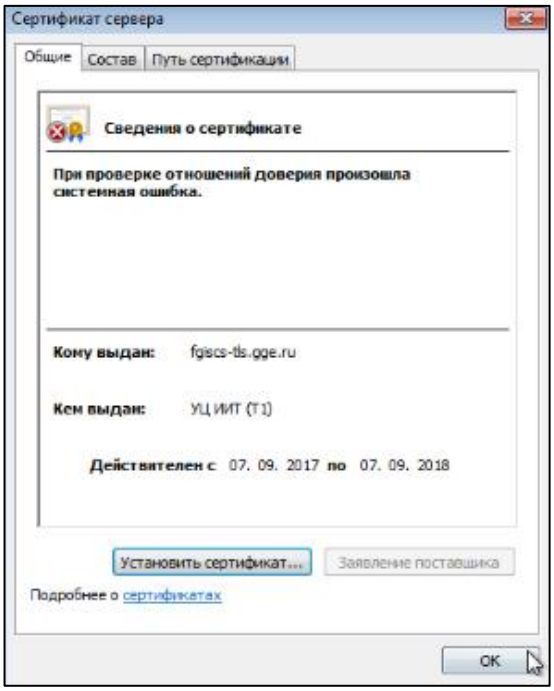

Рисунок 67 – Окно «Сертификат сервера»

21) в окне «Шаг 2. Укажите сертификат сервера» нажмите кнопку «Далее» (Рисунок 68);

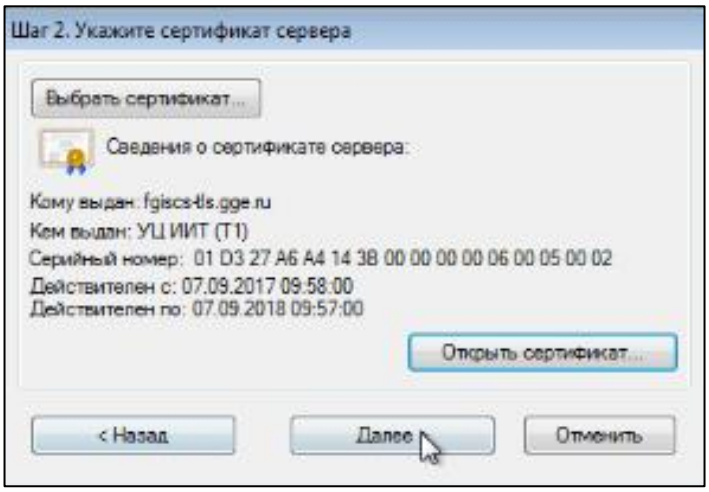

Рисунок 68 – Окно «Шаг 2. Укажите сертификат сервера»

22) в окне «Шаг 3. Выбрать сертификат издателя» нажмите кнопку «Выбрать сертификат» (Рисунок 69);

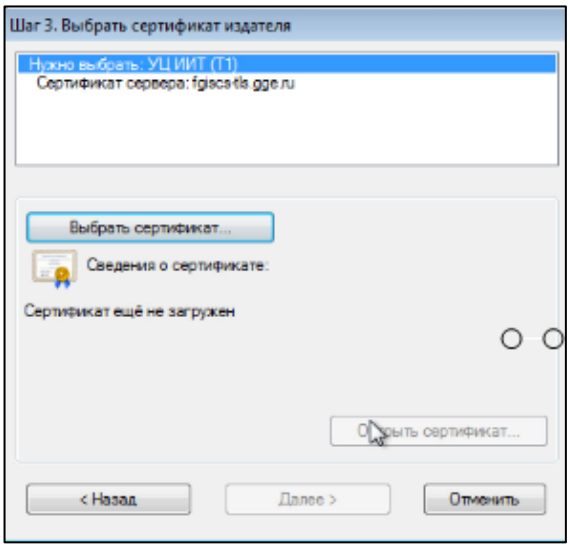

Рисунок 69 – Окно «Шаг 3. Выбрать сертификат издателя»

23) укажите путь к сертификату, выданному Удостоверяющим центром в комплекте ПО «Континент TLS VPN» (файл **уц иит т1 (1).cer**) (Рисунок 70);

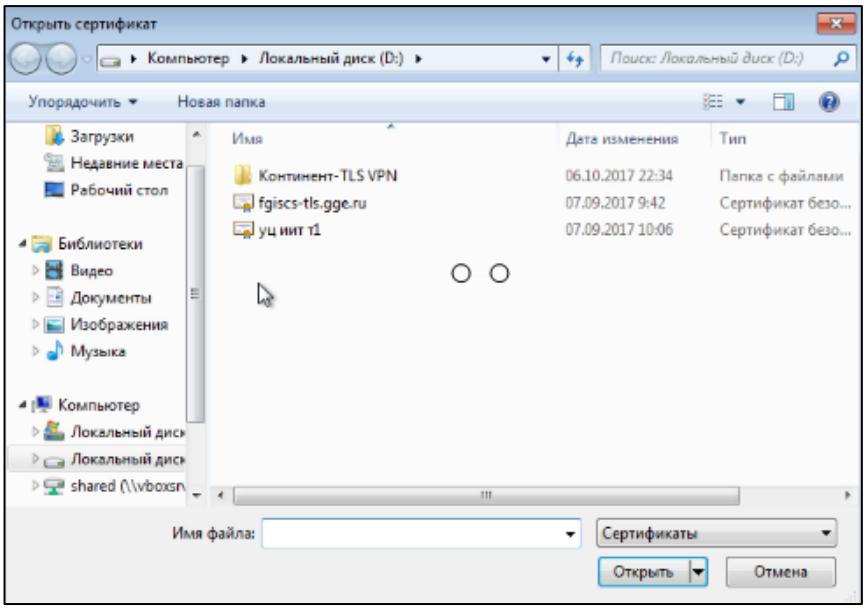

Рисунок 70 – Открытие сертификата Удостоверяющего центра

24) выделите сертификат, нажмите кнопку «Открыть сертификат» (Рисунок 71);

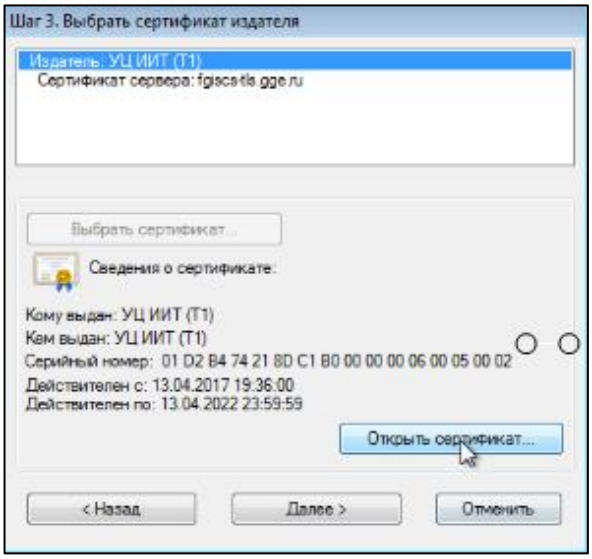

Рисунок 71 – Выбор сертификата Удостоверяющего центра

25) в окне «Сертификат» нажмите кнопку «Установить сертификат» (Рисунок 72);

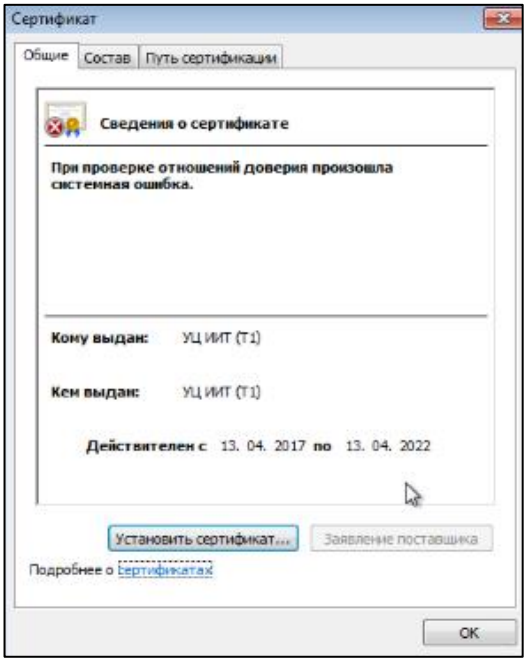

Рисунок 72 – Окно «Сертификат»

26) в окне «Мастер импорта сертификатов» нажмите кнопку «Далее» (Рисунок 73).

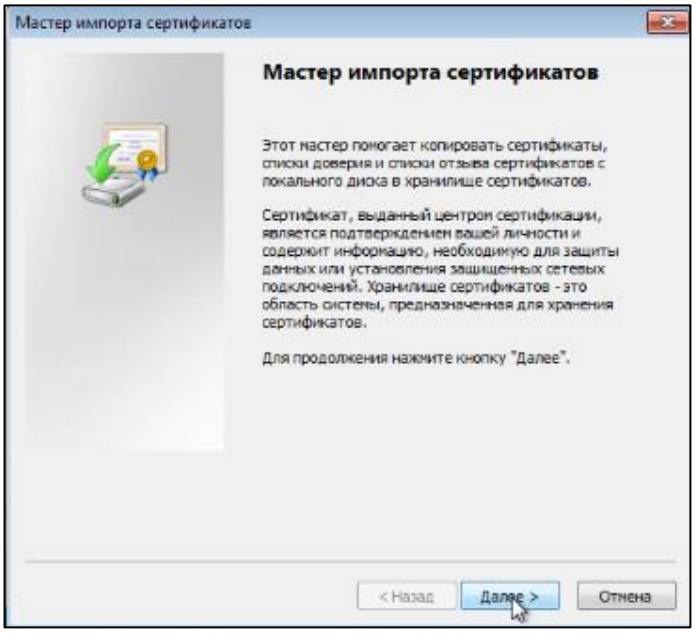

Рисунок 73 – Кнопка «Далее»

27) установите переключатель на параметр «Автоматически выбирать хранилище на основе типа сертификата», нажмите кнопку «Далее» (Рисунок 74);

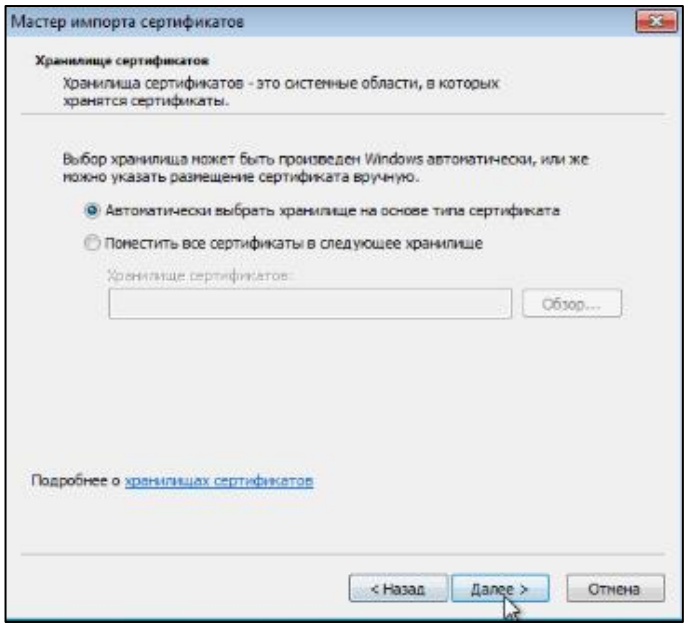

Рисунок 74 – Выбор параметра «Автоматически выбирать хранилище на основе типа сертификата»

28) в окне «Завершение мастера импорта сертификатов» нажмите кнопку «Готово» (Рисунок 75);

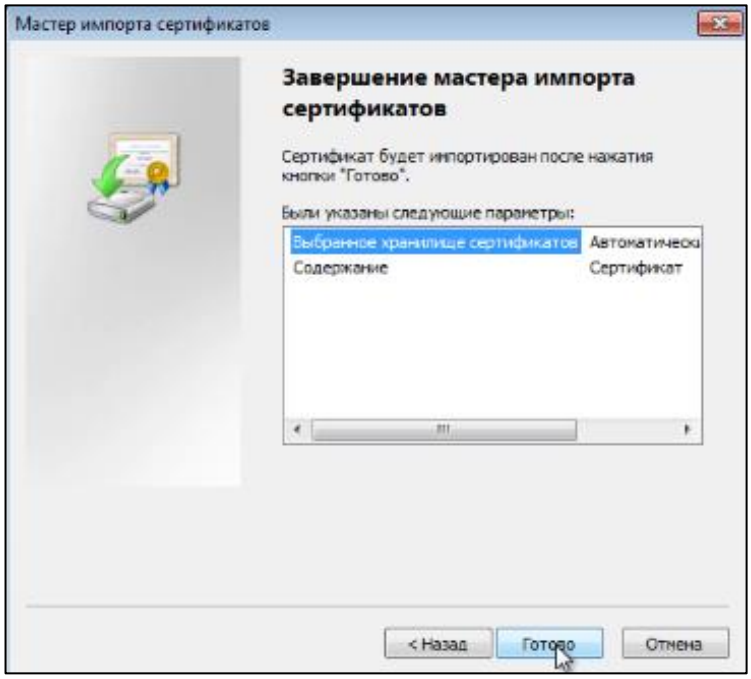

Рисунок 75 – Окно «Завершение мастера импорта сертификатов»

29) в окне с сообщением «Импорт успешно выполнен» нажмите кнопку «ОК» (Рисунок 76);

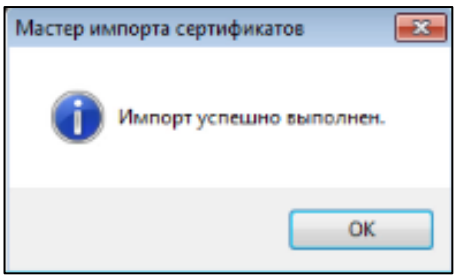

Рисунок 76 – Сообщение «Импорт успешно выполнен»

30) в окне «Шаг 3. Выбрать сертификат издателя» нажмите кнопку «Далее» (Рисунок 77);

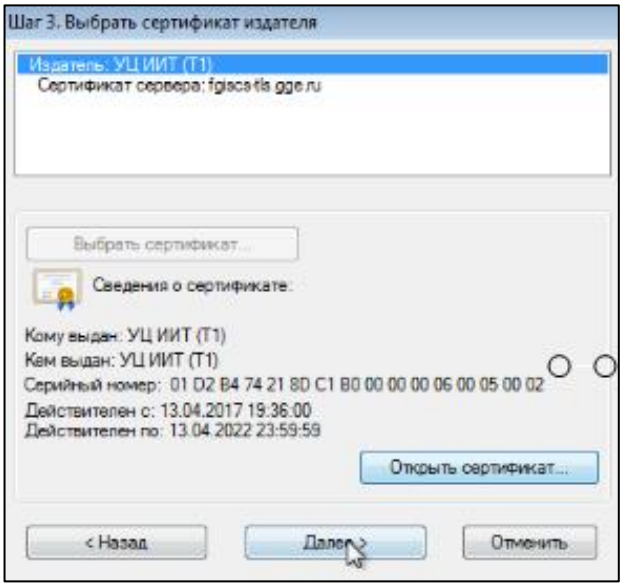

Рисунок 77 – Окно «Шаг 3. Выбрать сертификат издателя»

31) отобразится окно «Шаг 4. Укажите адрес получения CRL списка». Действия по настройке в данном окне выполнять не требуется, нажмите кнопку «Далее» (Рисунок 78);

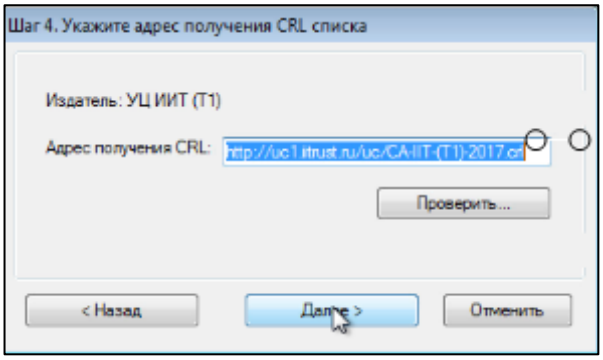

Рисунок 78 – Окно «Шаг 4. Укажите адрес получения CRL списка»

32) в окне «Создание защищенного соединения завершено» нажмите кнопку «ОК» (Рисунок 79);

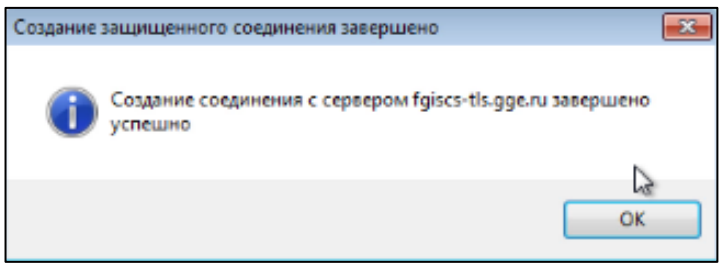

Рисунок 79 – Окно «Создание защищенного соединения завершено»

33) в окне «Настройки Континент TLS Клиента КС1» нажмите кнопку «Сохранить» (Рисунок 80);

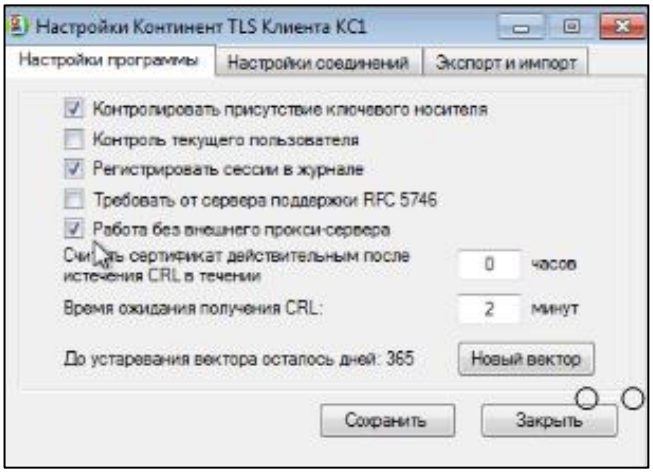

Рисунок 80 – Окно «Настройки Континент TLS Клиента КС1»

34) отобразится информационное окно с сообщением: «Адрес 127.0.0.1:8080 установлен как системный прокси-сервер». Нажмите кнопку «ОК» (Рисунок 81);

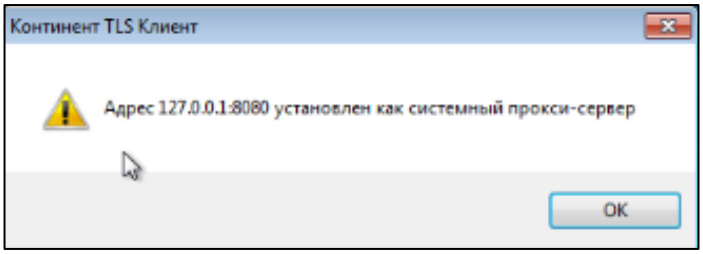

Рисунок 81 – Информационное сообщение

Отобразится информационное окно с сообщением: «Настройки программы успешно сохранены» (Рисунок 82).

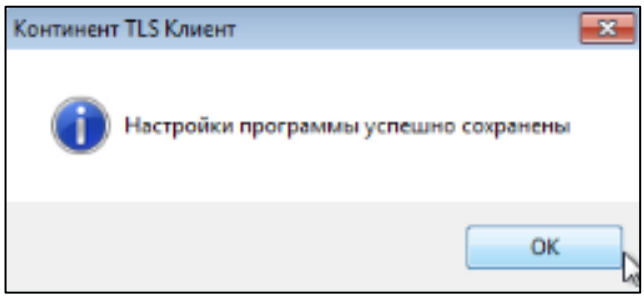

Рисунок 82 – Информационное сообщение

35) проверьте настройки прокси-сервера:

- нажмите кнопку «Пуск»;
- нажмите кнопку «Панель управления»;
- выберите раздел «Свойства браузера». На экране появится окно «Свойства: Интернет» (Рисунок 83);

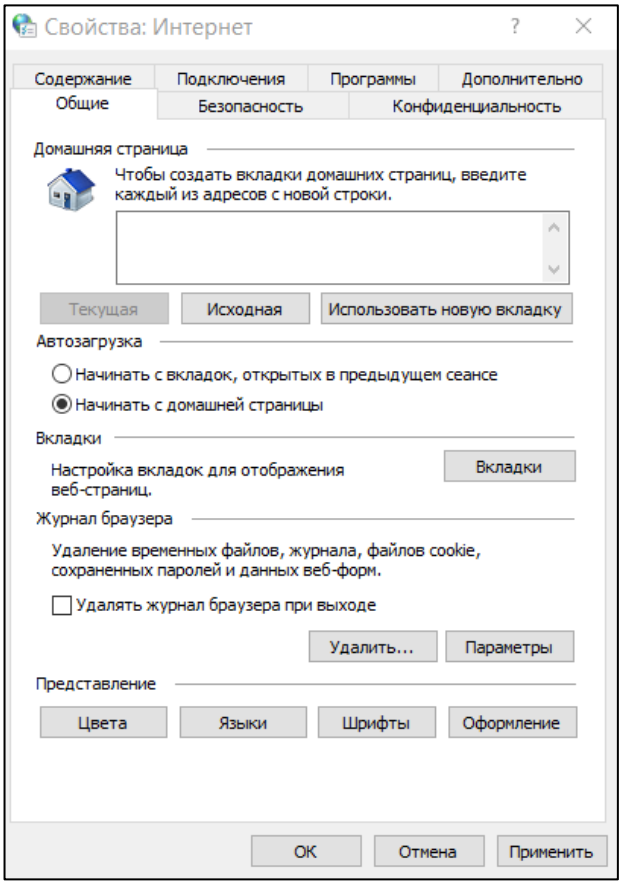

Рисунок 83 – Окно «Свойства: Интернет»

– перейдите во вкладку «Подключения», затем нажмите кнопку «Настройка сети» (Рисунок 84);
– убедитесь, что настройка «Использовать прокси-сервер для локальных подключений» разрешена;
– проверьте значения: в поле «Адрес» должно быть значение «127.0.0.1», в поле «Порт» – «8080».

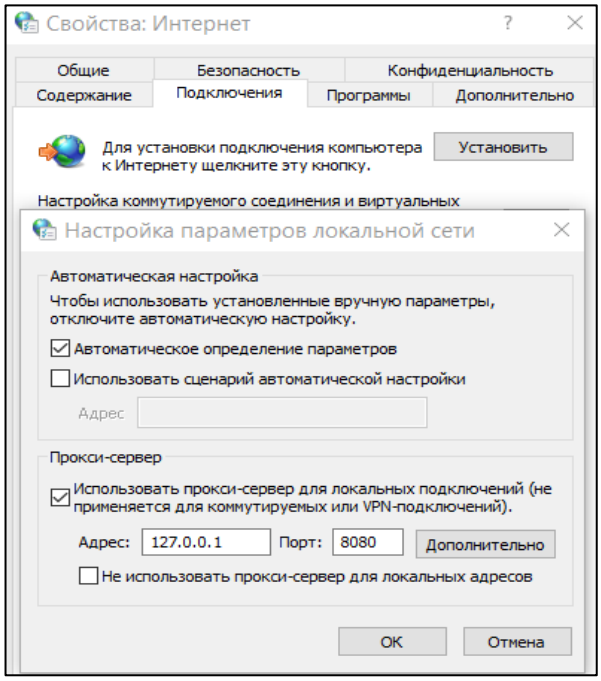

Рисунок 84 – Настройки прокси-сервера

– далее дважды последовательно нажмите кнопки «ОК».

Для проверки защищенного соединения с сервером выполните следующие действия:

1) откройте web-браузер, например, «Google Chrome»;
2) введите адрес сервера https://fgiscs-tls.gge.ru:8443 в адресной строке браузера и нажмите клавишу «Enter»;
3) убедитесь, что криптоконтейнер в виде внешнего носителя, полученный в комплекте усиленной квалифицированной электронной подписи в удостоверяющем центре Минкомсвязи России, подключен к компьютеру.

На экране появится окно «Континент TLS VPN» (Рисунок 53), в котором выберите хранилище (внешний носитель), действующий сертификат пользователя и введите пароль криптоконтейнера, полученные в комплекте УКЭП.

4) выберите хранилище, в котором хранится криптоконтейнер (Рисунок 85);

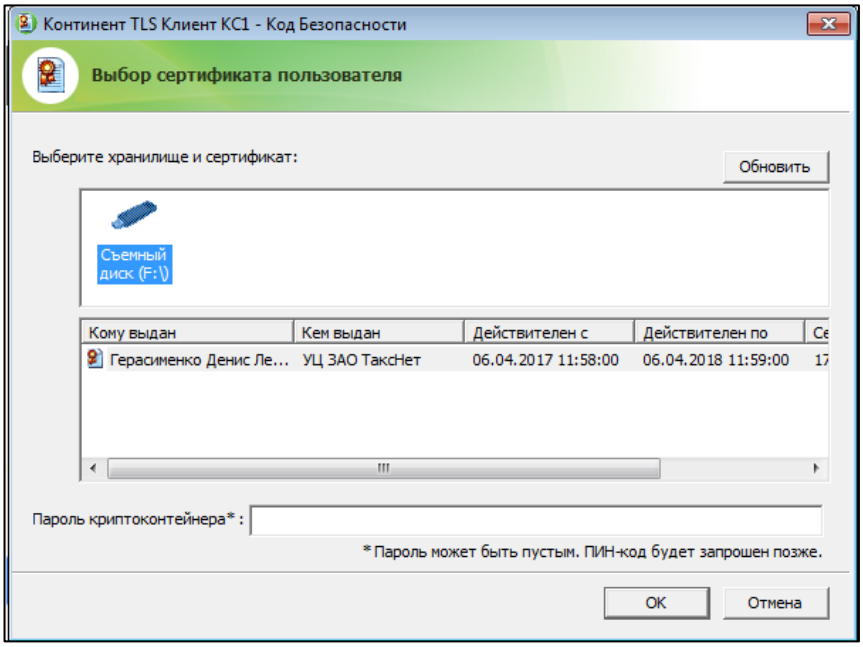

Рисунок 85 – Окно «Континент TLS VPN» для выбора хранилища

5) выберите действующий сертификат пользователя (Рисунок 86);

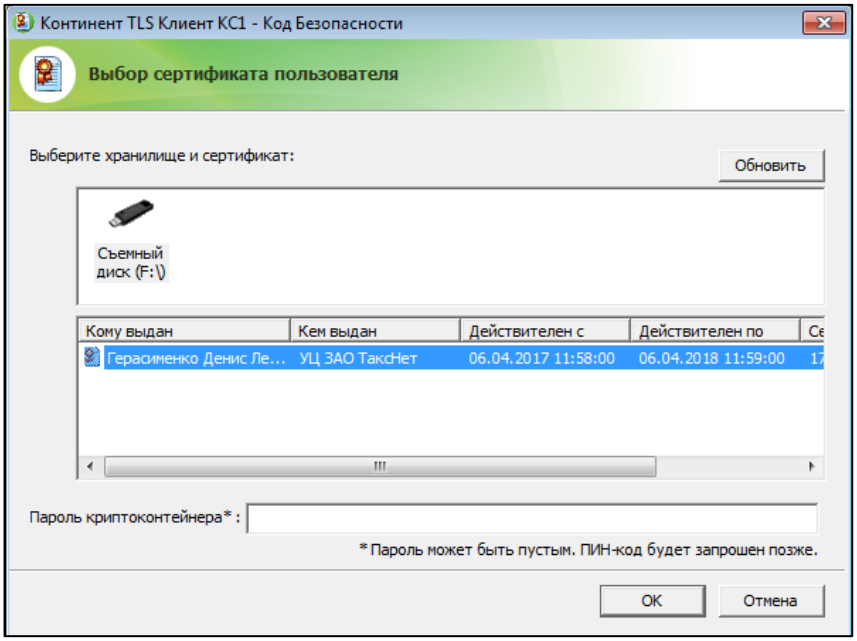

Рисунок 86 – Окно «Континент TLS VPN» выбора действующего сертификата пользователя

6) введите пароль криптоконтейнера, полученный в комплекте УКЭП (Рисунок 87);

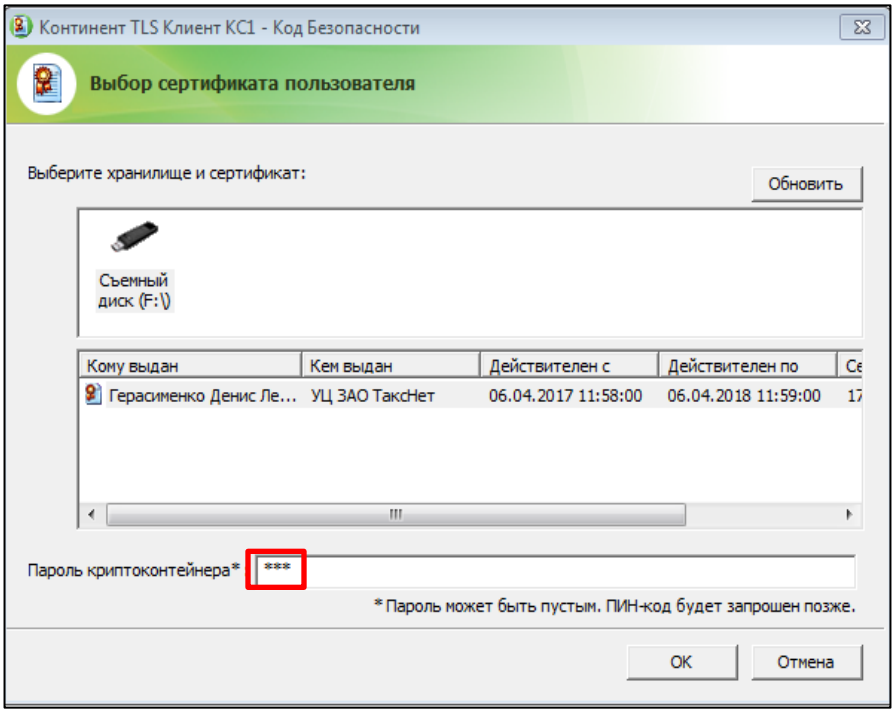

Рисунок 87 – Окно «Континент TLS VPN» с введенным паролем криптоконтейнера

Обратите внимание, что после ввода пароля криптоконтейнера пиктограмма программного обеспечения «Континент TLS VPN» (Рисунок 88), размещенная в правом нижнем углу панели рабочего стола, изменит свой цвет с красного («не подключен») на зеленый («подключен») (Рисунок 89).

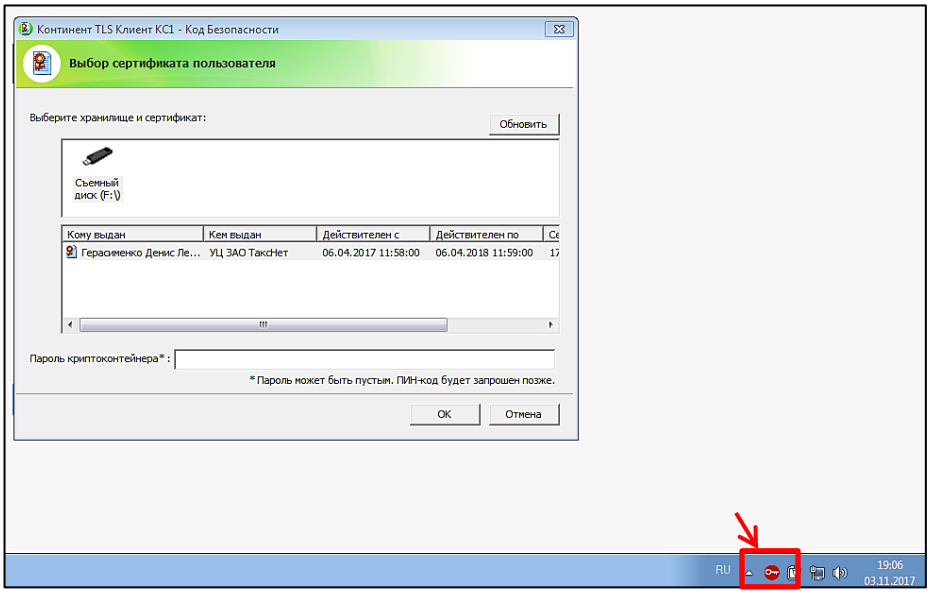

Рисунок 88 – Окно рабочего стола, красная пиктограмма «Континент TLS VPN»

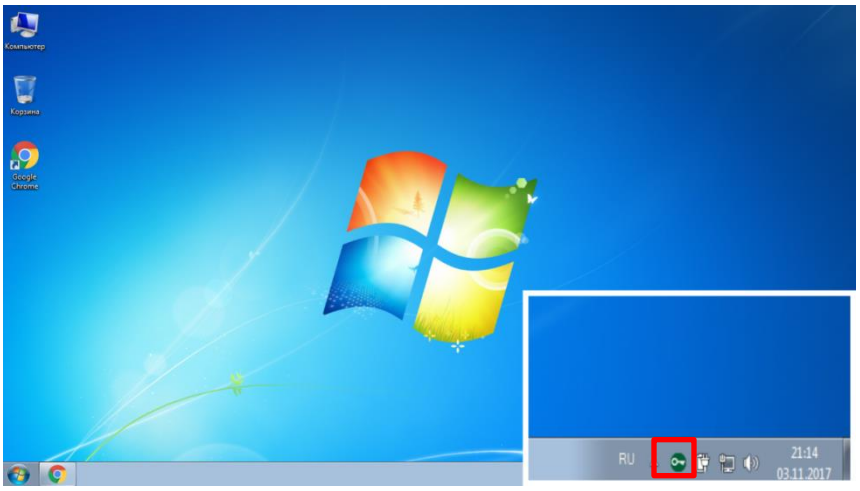

Рисунок 89 – Окно рабочего стола, зеленая пиктограмма «Континент TLS VPN»

На экране появится страница с сообщением «Ваше подключение не защищено» (Рисунок 90). Выполните необходимые действия, чтобы обеспечить переход на Портал ФГИС ЦС и дальнейшую работу с Порталом ФГИС ЦС через защищенное соединение, для этого:

1) нажмите на кнопку «Дополнительные» (Рисунок 90);

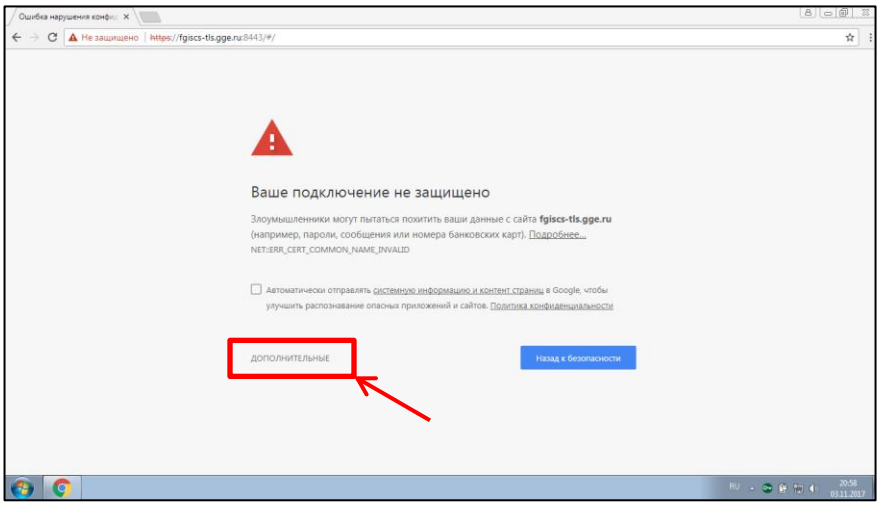

Рисунок 90 – Окно web-браузера «Google Chrome» для перехода на Портал ФГИС ЦС

2) в дополнительных сведениях перейдите по ссылке «Перейти на сайт fgiscs-tls.gge.ru» (Рисунок 91).

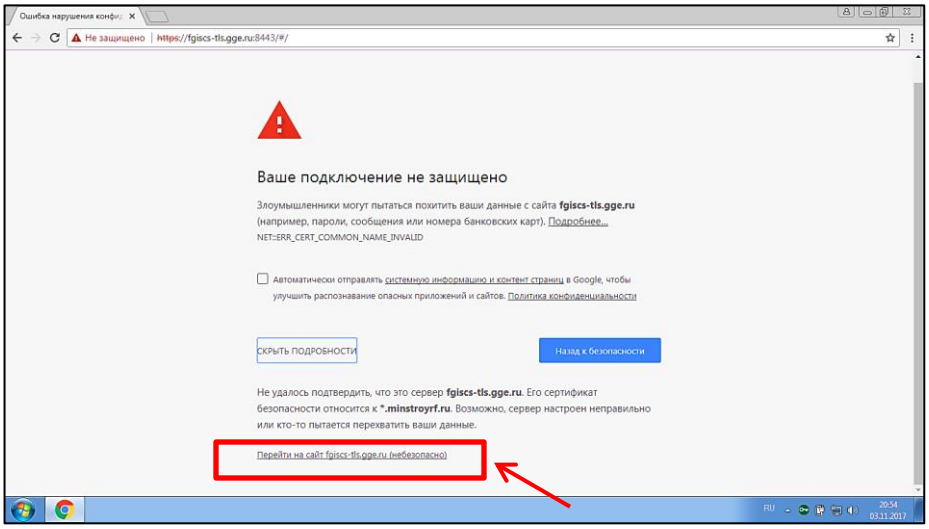

Рисунок 91 – Окно для перехода на Портал ФГИС ЦС

3) перейдите по ссылке «Перейти на сайт fgiscs-tls.gge.ru» на экране (Рисунок 58).
4) выполните вход в личный кабинет ФГИС ЦС (см. п. 8).

Установка и настройка ПО «Континент TLS VPN» завершена.

8 Вход в личный кабинет ФГИС ЦС

Для входа в личный кабинет ФГИС ЦС выполните следующие шаги:

1) откройте web-браузер, например, «Google Chrome»;
2) перейдите на Портал ФГИС ЦС по ссылке: fgiscs.minstroyrf.ru/;
3) нажмите на кнопку «Личный кабинет», отображаемую в виде ссылки (Рисунок 92);
4) для авторизации в личном кабинете ФГИС ЦС вы будете перенаправлены на портал ЕСИА.

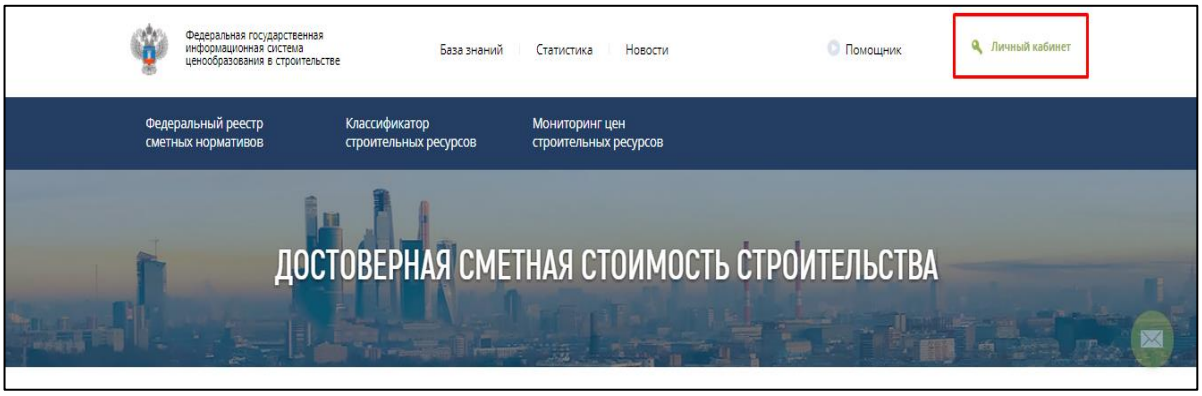

Рисунок 92 – Кнопка «Личный кабинет»