Федеральная государственная

информационная система ценообразования в строительстве

(ФГИС ЦС)

Инструкция по входу в личный кабинет ФГИС ЦС

2018

Аннотация

Уважаемые пользователи федеральной государственной информационной системы ценообразования в строительстве!

Данная инструкция описывает порядок получения доступа к личному кабинету федеральной государственной информационной системы ценообразования в строительстве (далее – ФГИС ЦС) и предназначена для:

- производителей строительных ресурсов на территории Российской Федерации;
- организаций, осуществляющих ввоз этих ресурсов в Российскую Федерацию для внутреннего потребления;
- перевозчиков строительных ресурсов;
- 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
DNS	Компьютерная распределённая система для получения информации о доменах
АРМ	Автоматизированное рабочее место
ГОСТ	Государственный стандарт
ЕСИА	Единая система идентификации и аутентификации, предназначена для формирования единых методов регистрации, идентификации и аутентификации пользователей во всех государственных информационных системах
КриптоПро CSP	Средство криптографической защиты информации КриптоПро CSP
Минкомсвязь РФ	Министерство связи и массовых коммуникаций Российской Федерации
ПК	Персональный компьютер
ПО	Программное обеспечение
ПО «Jinn-Client»	Сертифицированное средство криптографической защиты информации для создания электронной подписи и доверенной визуализации документов
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»
Протокол RDP	Протокол удалённого рабочего стола
СКЗИ	Средство криптографической защиты информации
СНИЛС	Страховой номер лицевого счета гражданина в системе обязательного пенсионного страхования
УКЭП	Усиленная квалифицированная электронная подпись
ФГИС ЦС	Федеральная государственная информационная система ценообразования в строительстве

Термин, сокращение	Определение
ФСБ России	Федеральная служба безопасности Российской Федерации

1 Общие положения

Для входа на Портал ФГИС ЦС сначала пройдите авторизацию на портале Госуслуг и получите усиленную квалифицированную электронную подпись (далее – УКЭП), которая понадобится для обеспечения юридической значимости передаваемых во ФГИС ЦС данных. УКЭП должна быть выдана одним из аккредитованных Удостоверяющих центров. Перечень аккредитованных Удостоверяющих центров доступен на официальном сайте Минкомсвязи РФ: http://e-trust.gosuslugi.ru/CA.

Для регистрации организации (см. п. 3) сначала зарегистрируйте физическое лицо (руководителя организации либо представителя организации, имеющего право действовать от имени организации без доверенности) (см. п. 2).

2 Порядок регистрации физического лица

Для регистрации физического лица выполните следующую последовательность действий:

- приготовьте паспорт и страховое свидетельство обязательного пенсионного страхования;
- перейдите на портал Госуслуг – откройте страницу регистрации на esia.gosuslugi.ru/registration/;
- заполните поля: «Фамилия», «Имя», «Мобильный телефон» или «Или электронная почта», нажмите кнопку «Зарегистрироваться»;
- подтвердите номер телефона или адрес электронной почты. В результате на адрес электронной почты будет выслан код подтверждения;
- откройте электронное письмо и перейдите по указанной в нем ссылке подтверждения;
- 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»;
- 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;
- выполните процедуру подтверждения личности – эта процедура предусматривает ввод персонального идентификатора, полученного лично одним из следующих доступных способов:
  - первый способ – личное обращение. Данный способ 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.

– перейдите к регистрации юридического лица (см. п. 3).

3 Порядок регистрации юридического лица

Порядок регистрации юридического лица:

– авторизуйтесь на портале Госуслуг (https://esia.gosuslugi.ru) под учетной записью физического лица и нажмите кнопку «Показать все личные данные» на вкладке «Персональная информация».

Примечание – Для создания учетной записи организации необходимо предварительное наличие средства УКЭП юридического лица. Для получения средства УКЭП обратитесь в один из аккредитованных Минкомсвязью РФ Удостоверяющих центров, указанных на сайте https://minsvyaz.ru/ru/activity/govservices/2/, следуя инструкциям сайта https://minsvyaz.ru/ru/appeals/faq/35/.

– подключите к компьютеру средство электронной подписи;

– 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;

– 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;

– 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 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. 4) и ПО «Континент TLS VPN» (см. п. 5).

4 Установка ПО «Jinn-Client»

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

– поместите установочный диск в устройство чтения компакт-дисков и запустите к исполнению файл «Setup» из директории CD дистрибутива (важно: не CD_Sable). (Рисунок 1);

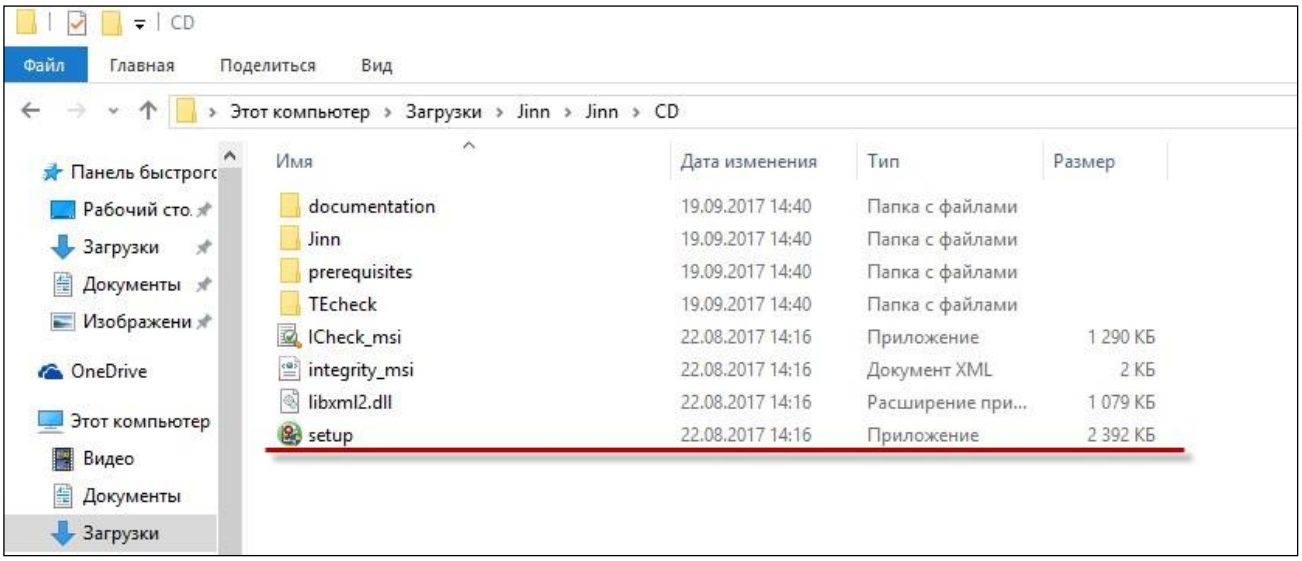

Рисунок 1 – Файл «Setup»

– на экране отобразится окно выбора компонента. Выберите пункт «Jinn-Client» (Рисунок 2);

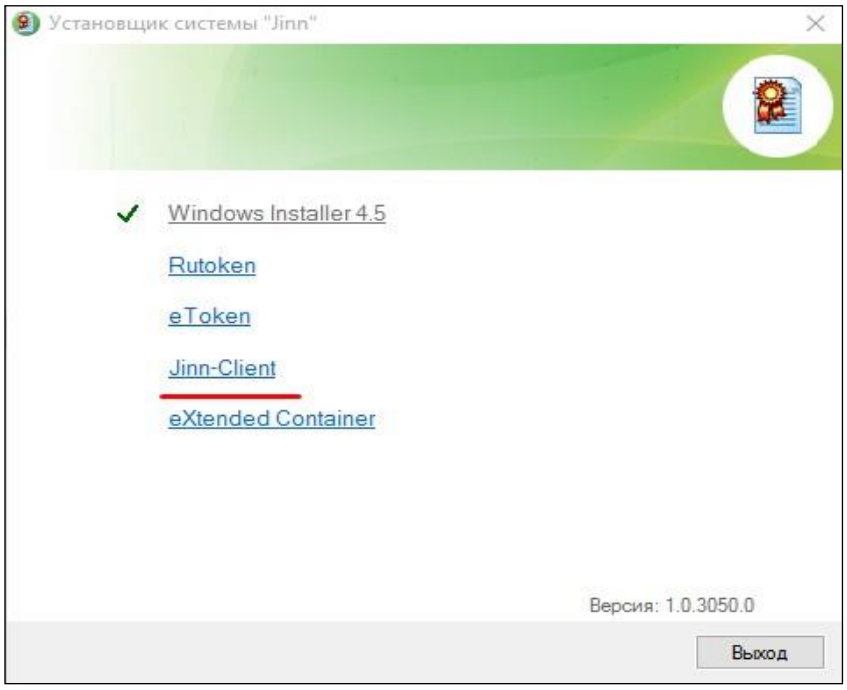

Рисунок 2 – Пункт «Jinn-Client»

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

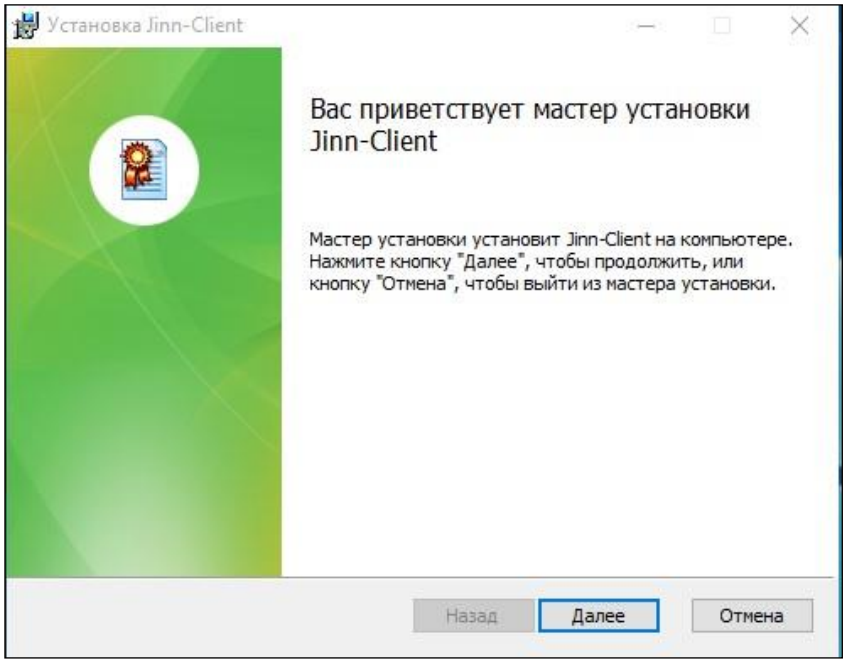

Рисунок 3 – Окно «Установка Jinn-Client»

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

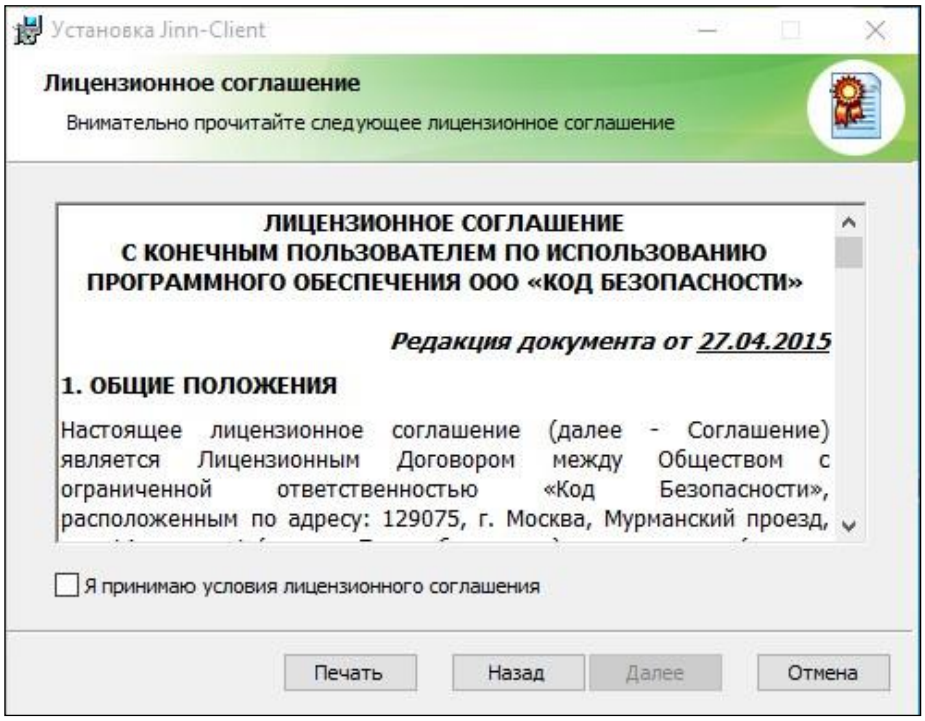

Рисунок 4 – Лицензионное соглашение

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

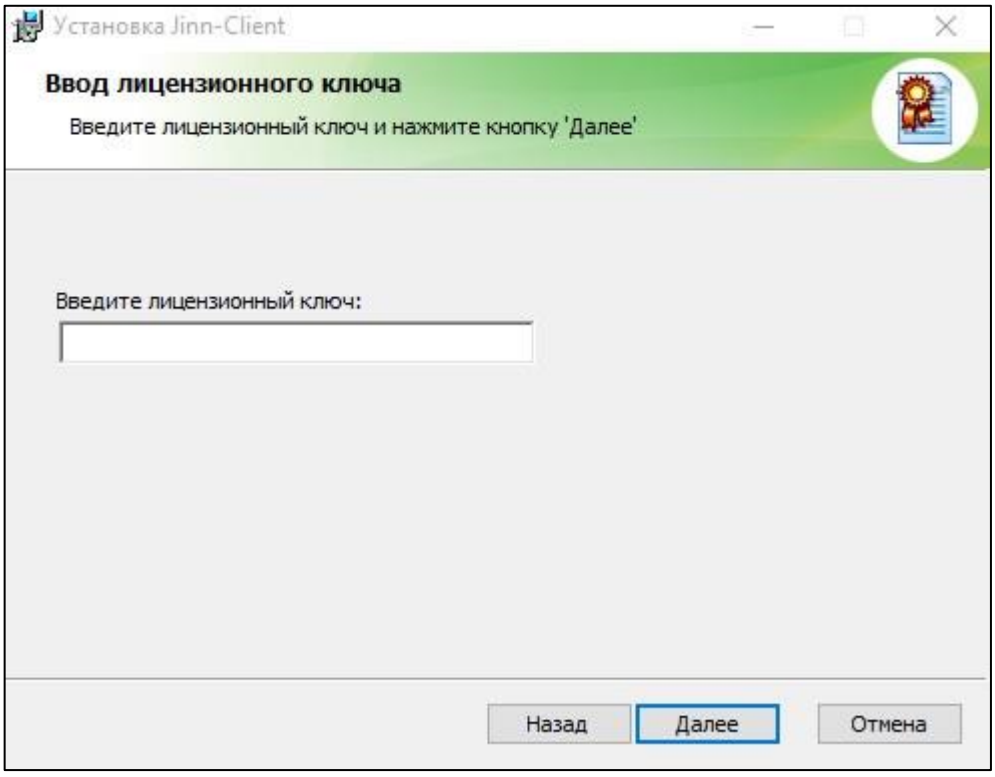

Рисунок 5 – Окно «Ввод лицензионного ключа»

– 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 6);

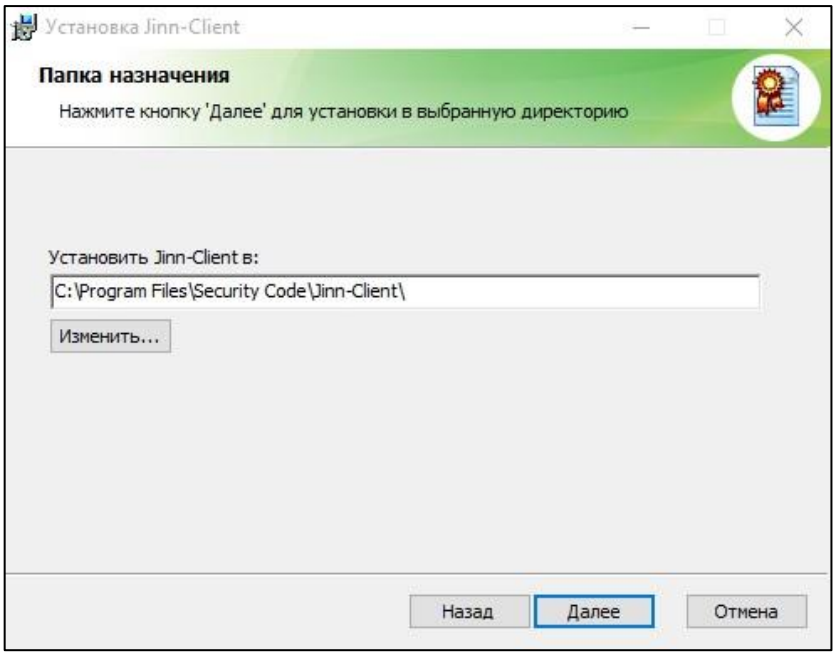

Рисунок 6 – Расположение каталога для разворачивания ПО «Jinn-Client»

– в окне «Настройка параметров «Jinn-Client»» нажмите кнопку «Далее» (Рисунок 7). Обратите внимание на то, что формирование доверенной среды не является обязательным для создания электронной подписи над документами во ФГИС ЦС;

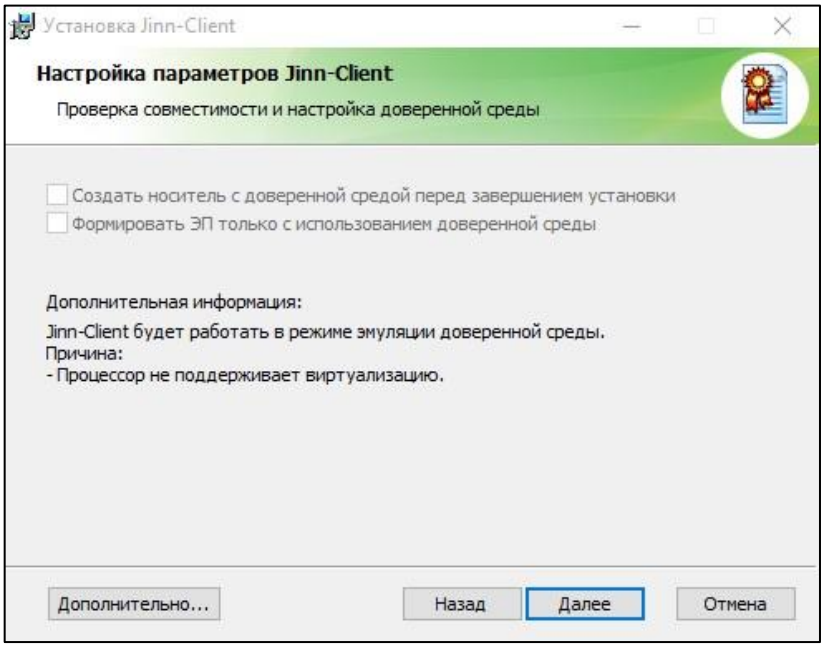

Рисунок 7 – Окно «Настройка параметров «Jinn-Client»

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

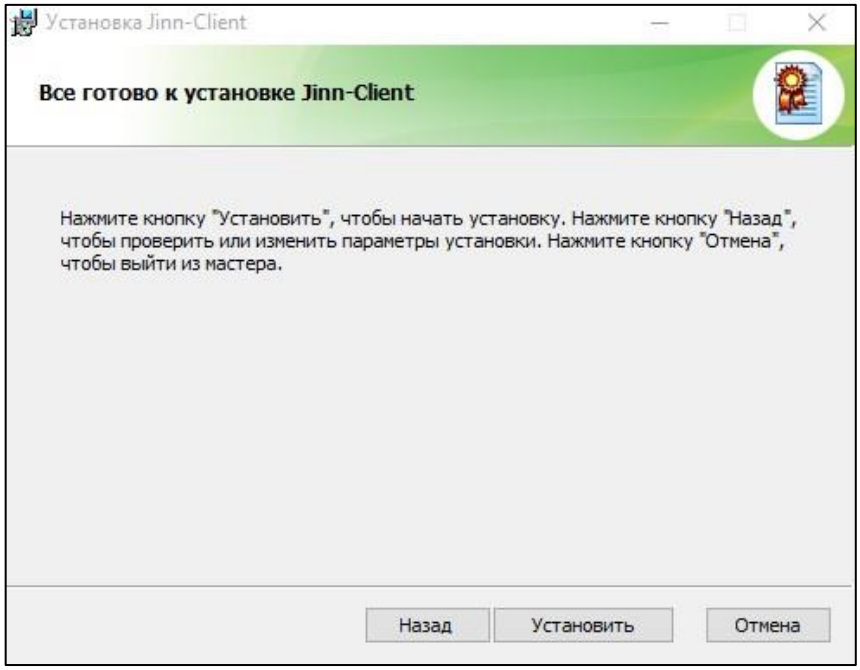

Рисунок 8 – Окно «Все готово к установке Jinn-Client»

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

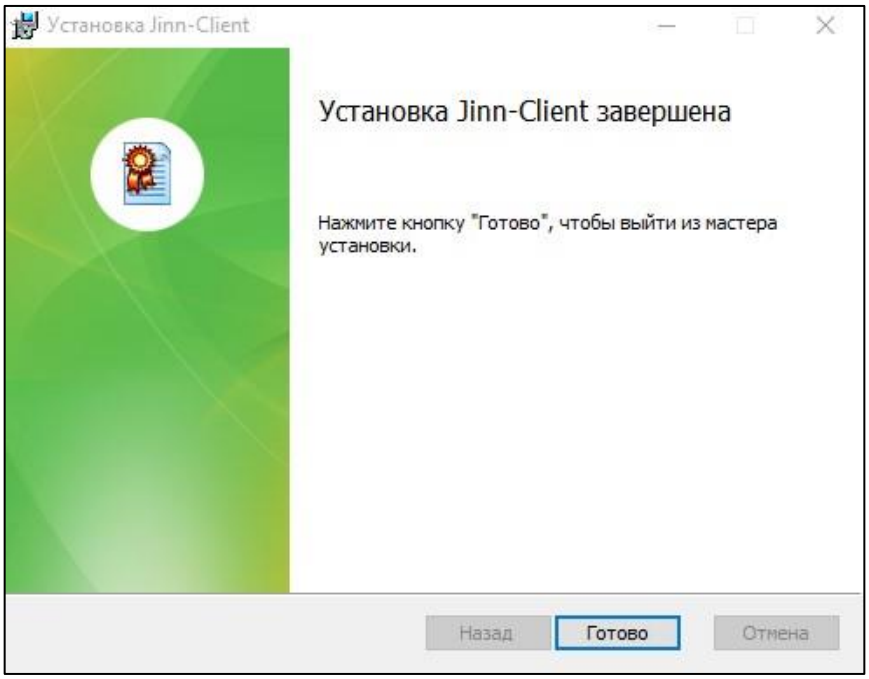

Рисунок 9 – Окно «Установка Jinn-Client завершена»

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

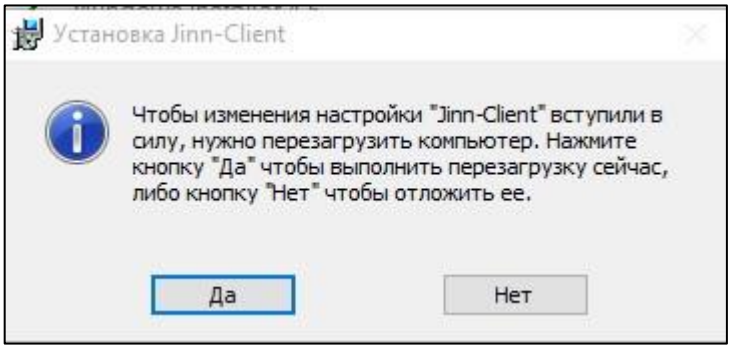

Рисунок 10 – Предложение перезагрузить компьютер

Для работы в web-браузере «Google Chrome» установите плагин «Jinn Sign Extension», для этого выполните следующую последовательность действий:

– перейдите в каталог дистрибутива «CD\prerequisites» и запустите установочный файл «JinnSignExtensionSetup.msi» (Рисунок 11);

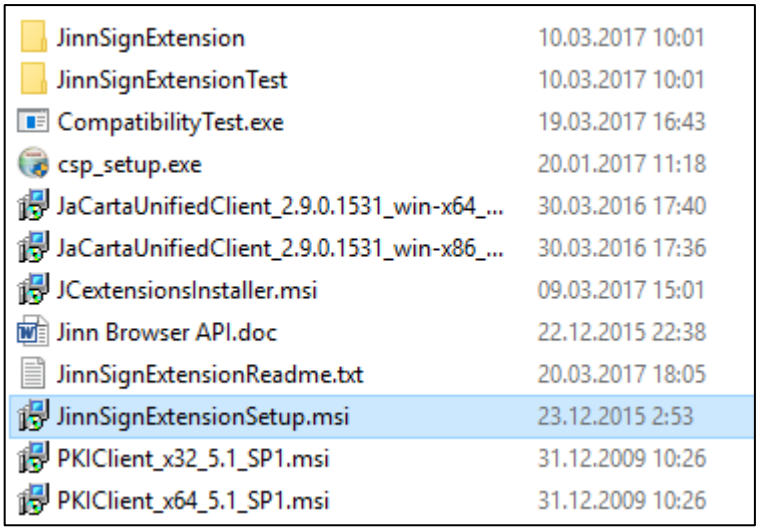

Рисунок 11 – «Установочный файл JinnSignExtensionSetup.msi»

– откроется окно приветствия мастера установки (Рисунок 12), нажмите кнопку «Далее»;

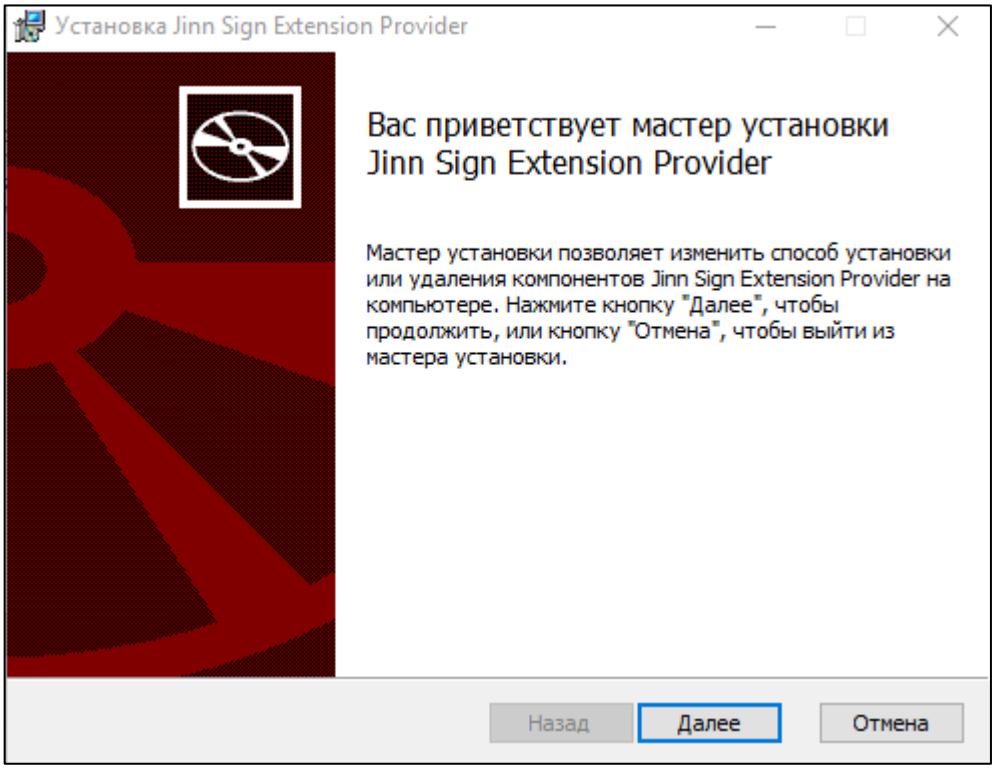

Рисунок 12 – Мастер установки ПО «Jinn Sign Extension Provider»

– ознакомьтесь с условиями лицензионного соглашения, установите «флажок» в поле «Я принимаю условия лицензионного соглашения», нажмите кнопку «Далее» (Рисунок 13);

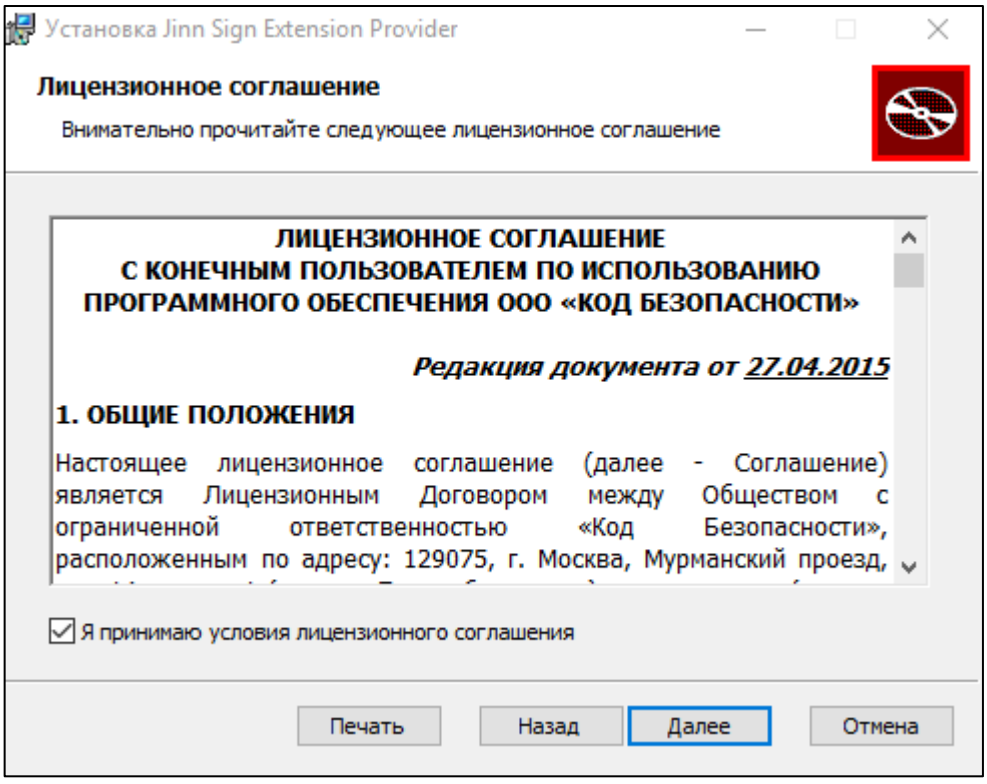

Рисунок 13 – Лицензионное соглашение использования ПО «Jinn Sign Extension Provider»

– оставьте путь инсталляции, установленный по умолчанию, нажмите кнопку «Далее» (Рисунок 14);

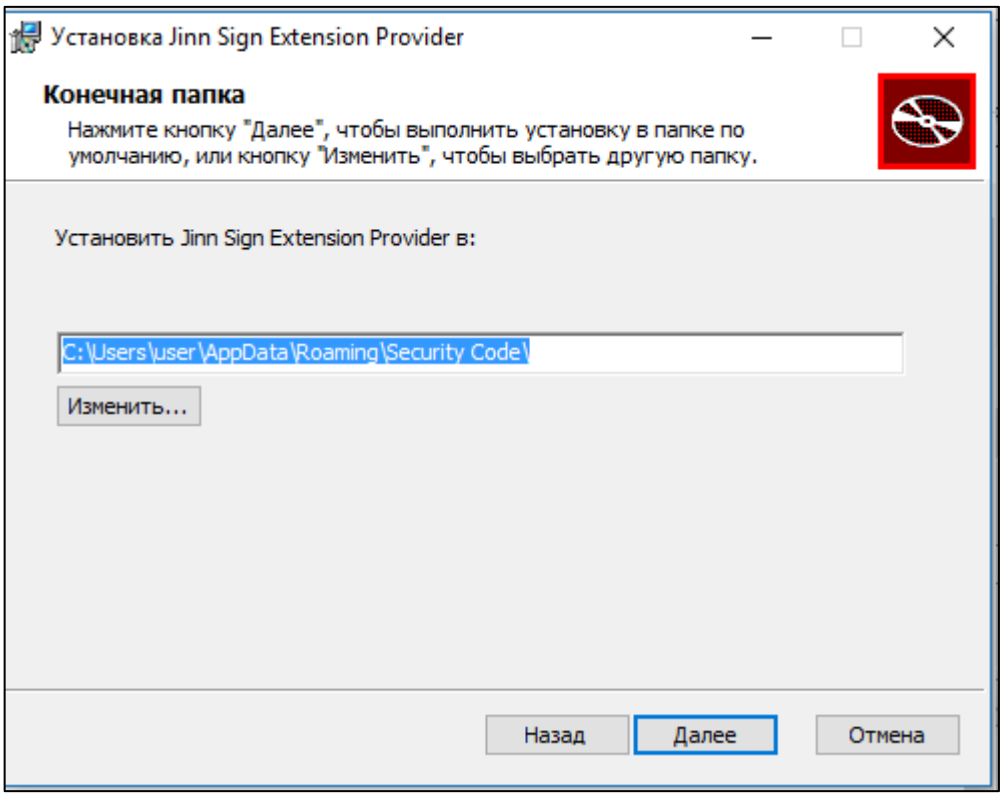

Рисунок 14 – Путь инсталляции ПО «Jinn Sign Extension Provider»

– далее нажмите кнопку «Установить» (Рисунок 15);

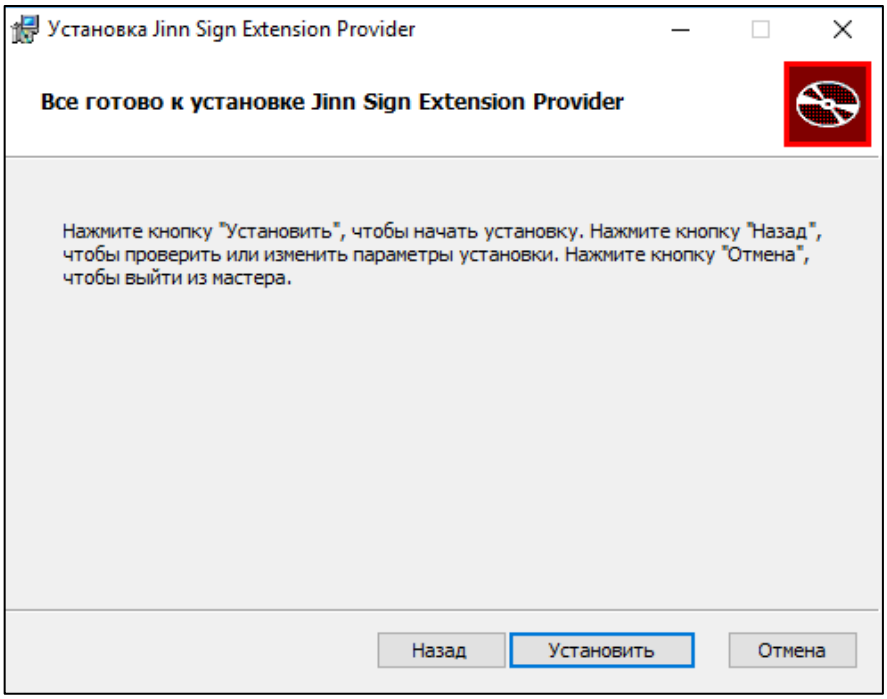

Рисунок 15 – Окно «Всего готово к установке Jinn Sign Extension Provider»

– убедитесь, что установка завершена успешно (Рисунок 16), нажмите кнопку «Готово» и перейдите к следующему пункту;

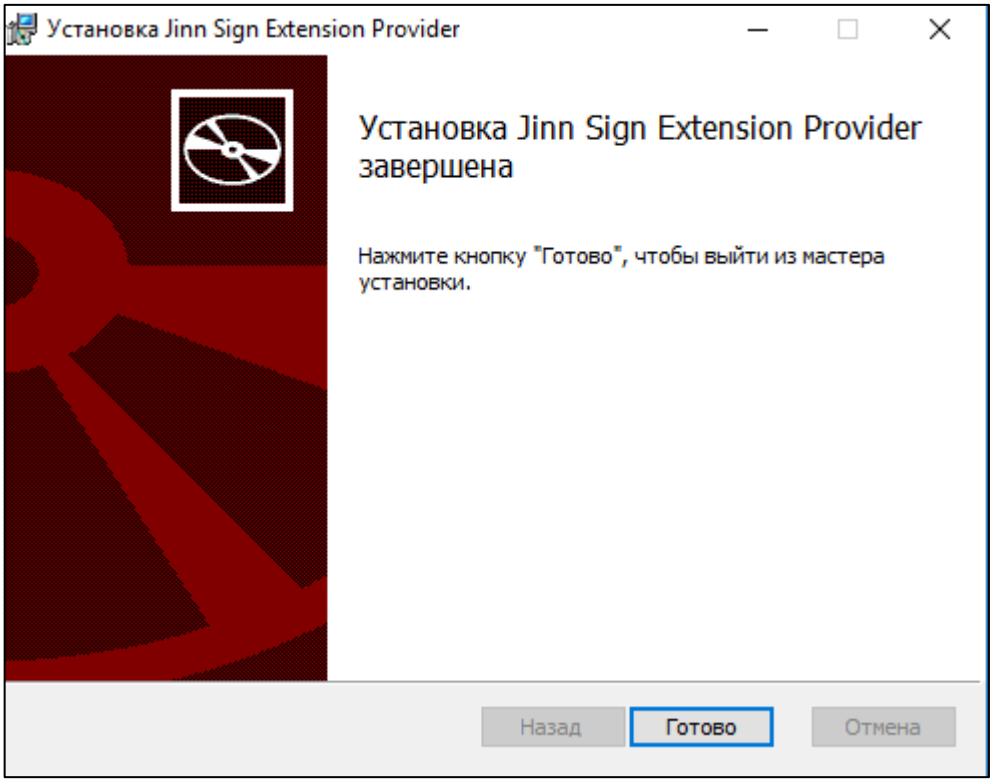

Рисунок 16 – Успешное завершение установки ПО «Jinn Sign Extension Provider»

– если установка завершена преждевременно (Рисунок 17), проверьте, отображается ли в окне «Программы и компоненты» (Пуск/Панель управления/Программы и компоненты) ПО «Jinn Sign Extension Provider»; если данное ПО отображается, то удалите его и установите заново, изменив директорию по умолчанию на «C:\Program Files(x86)\Security Code\»;

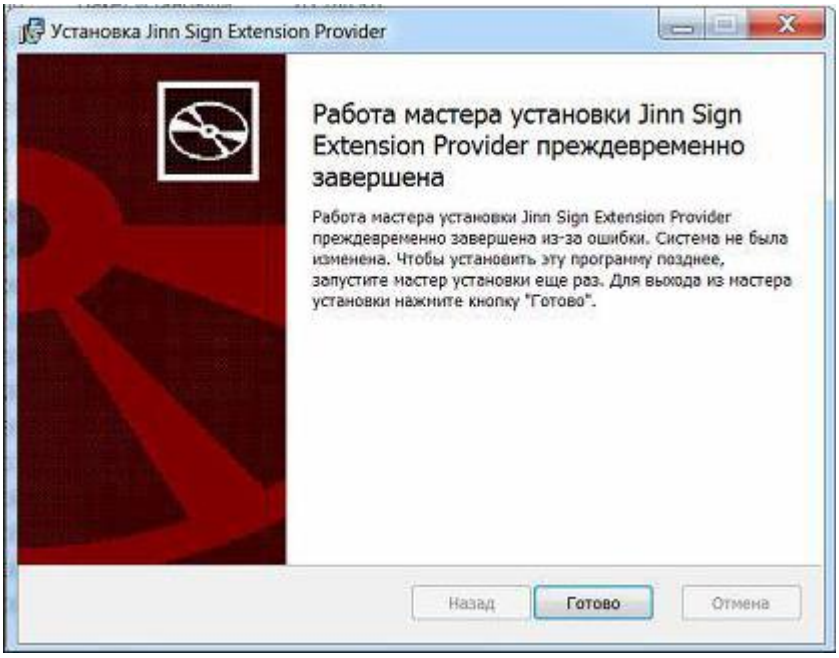

Рисунок 17 – Преждевременное завершение установки ПО «Jinn Sign Extension Provider»

– откройте web-браузер, нажмите кнопку вызова меню настроек и управления web-браузером. Выберите пункт «Дополнительные инструменты», затем пункт «Расширения» (Рисунок 18);

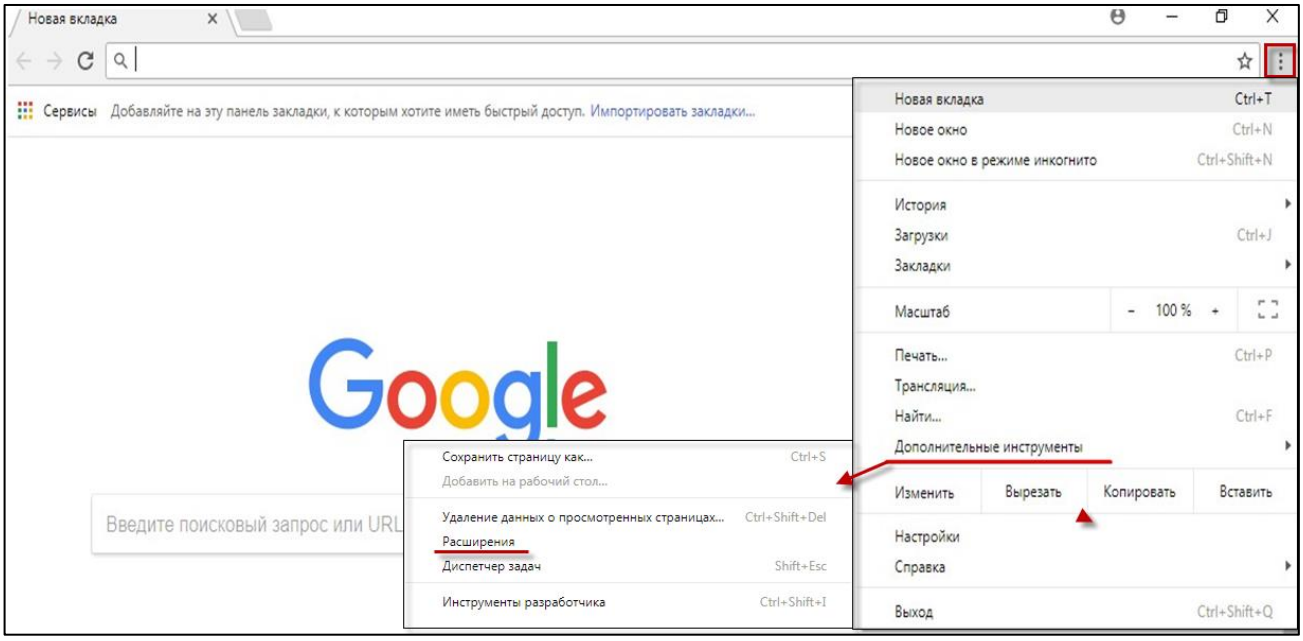

Рисунок 18 – Пункт «Дополнительные инструменты/Расширения»

– в окне «Расширения» выберите пункт «Еще расширения» (Рисунок 19);

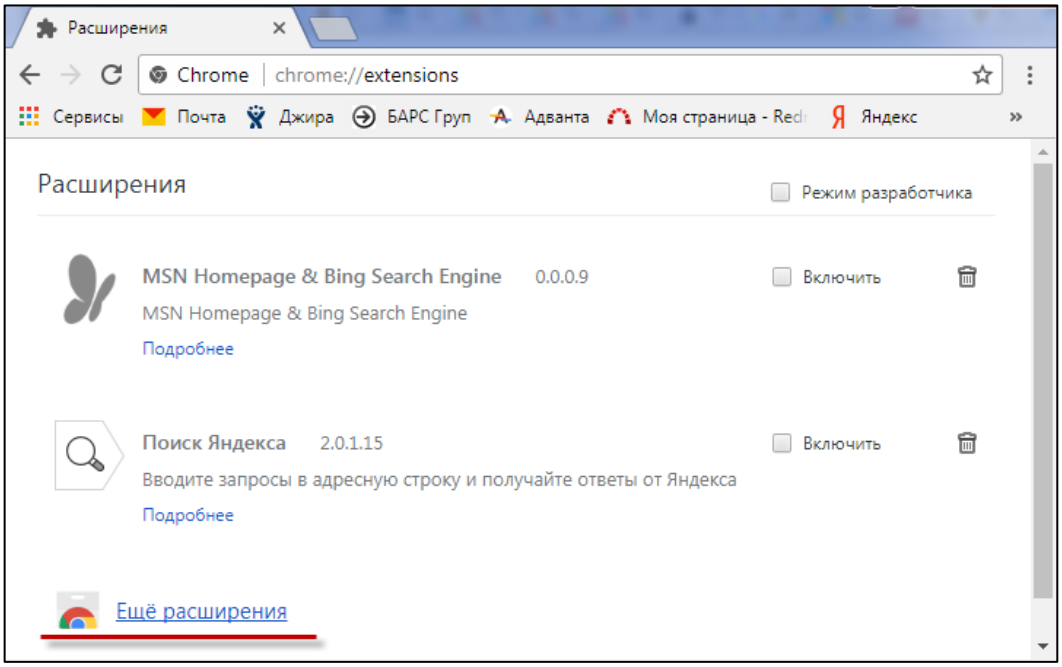

Рисунок 19 – Пункт «Еще расширения»

– отобразится окно «Интернет-магазин Chrome». В строку поиска введите значение «jinn», в предложенном списке выберите значение «jinn sign extension». Убедитесь в том, что программный продукт, который нужно установить, с ресурса www.securitycode.ru – отображается надпись «предлагается на сайте www.securitycode.ru» (Рисунок 20);

Рисунок 20 – ПО «Jinn Sign Extension» с ресурса www.securitycode.ru

– нажмите кнопку «Установить»;
– отобразится окно «Установить «Jinn Sign Extension»?», нажмите кнопку «Установить расширение» (Рисунок 21);

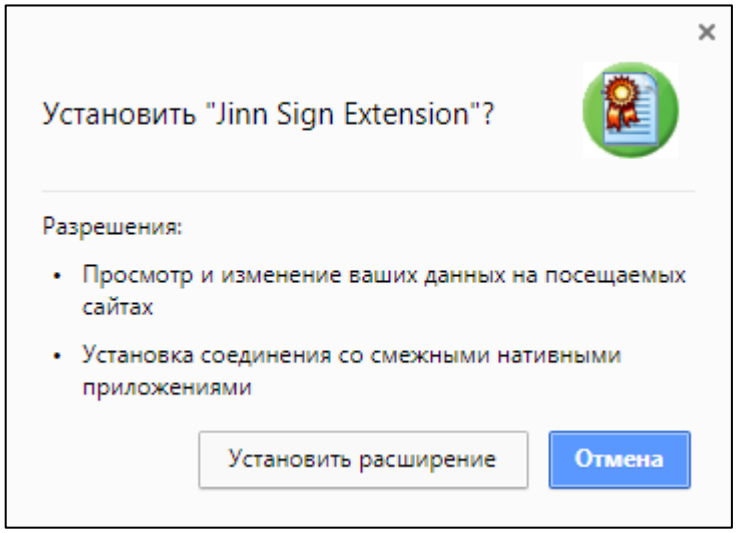

Рисунок 21 – Окно «Установить «Jinn sign Extension»?»

– после установки расширения вернитесь в раздел «Расширения», найдите информацию о «Jinn Sign Extension» и установите «флажок» в поле параметра «Разрешить открывать локальные файлы по ссылкам» (Рисунок 22).

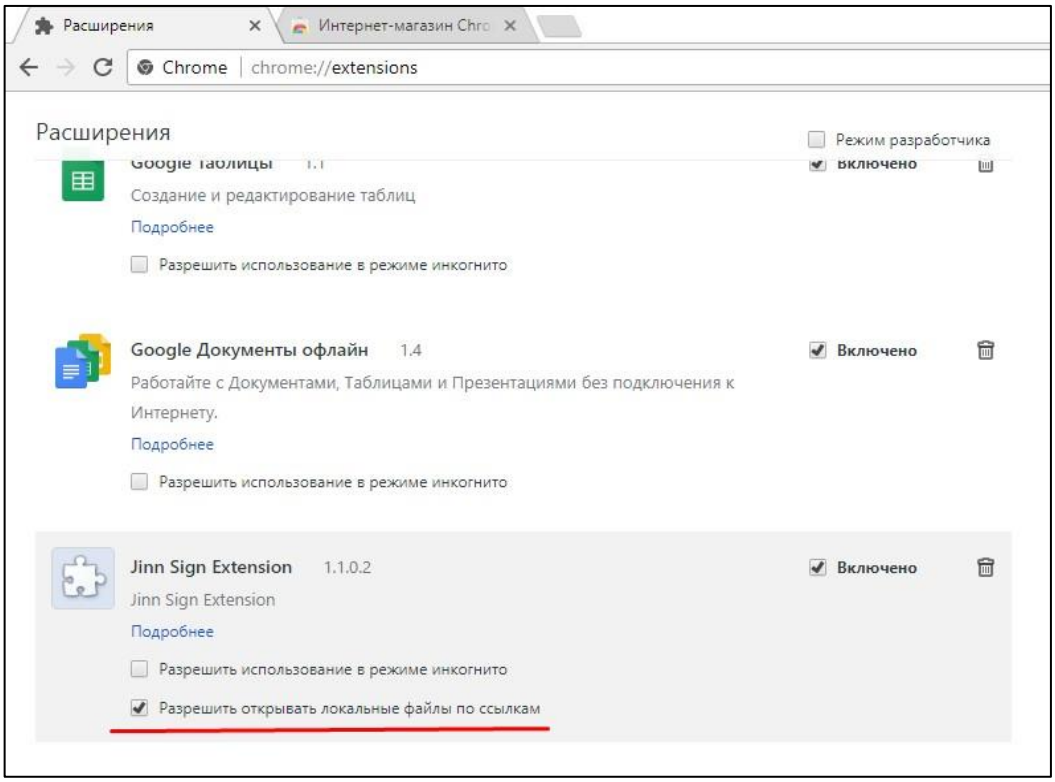

Рисунок 22 – Назначение параметра «Разрешить открывать локальные фалы по ссылкам»

Установка и настройка ПО«Jinn Sign Extension» завершена.

5 Установка ПО «Континент TLS VPN»

5.1 Предварительные требования

Для доступа в личный кабинет ФГИС ЦС между АРМ пользователя и ресурсом https://fgiscs-tls.gge.ru:8443 (для получения сетевого адреса воспользуйтесь публичным DNS) должны быть открыты следующие порты: tcp 80, tcp 443, tcp 8443.

Если доступ к сети Интернет осуществляется через устройство, фильтрующее сетевой трафик, описанные правила должны быть настроены на данном оборудовании сотрудником, выполняющим роль системного администратора.

Для проверки наличия сетевого доступа до установки ПО «Континент TLS VPN» выполните в командной строке последовательно команды:

- telnet fgiscs-tls.gge.ru 8443;
- telnet fgiscs-tls.gge.ru 443;
- telnet fgiscs-tls.gge.ru 80.

Предварительно установите клиент «Telnet». Нажмите кнопку «Пуск» и перейдите в раздел «Панель управления/ Программы и компоненты/ Включение или отключение компонентов Windows». В открывшемся окне установите «флажок» напротив значения «Клиент Telnet», нажмите кнопку «ОК» и дождитесь установки. Признаком успешного выполнения команды является наличие мигающего курсора в командной строке.

Также для ресурса https://fgiscs-tls.gge.ru:8443 не должна производиться подмена сертификата сервера на промежуточном оборудовании между АРМ пользователя и конечным ресурсом.

Обратите внимание, что установка и работа с ПО «Континент TLS VPN» по протоколу RDP технически невозможна, по требованиям ФСБ России все действия должны выполняться исключительно локально.

До начала установки ПО «Континент TLS VPN» загрузите сертификаты «Сертификат Удостоверяющего Центра» и «Сертификат сервера для ПО «Континент TLS VPN» с официального сайта https://fgiscs.minstroyrf.ru/#/educationalMaterial в любую локальную директорию АРМ.

5.2 Инсталляция ПО «Континент TLS VPN»

Для 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. Для этого выполните следующие действия:

– поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл «ContinentTLSSetup.exe» (Рисунок 23);

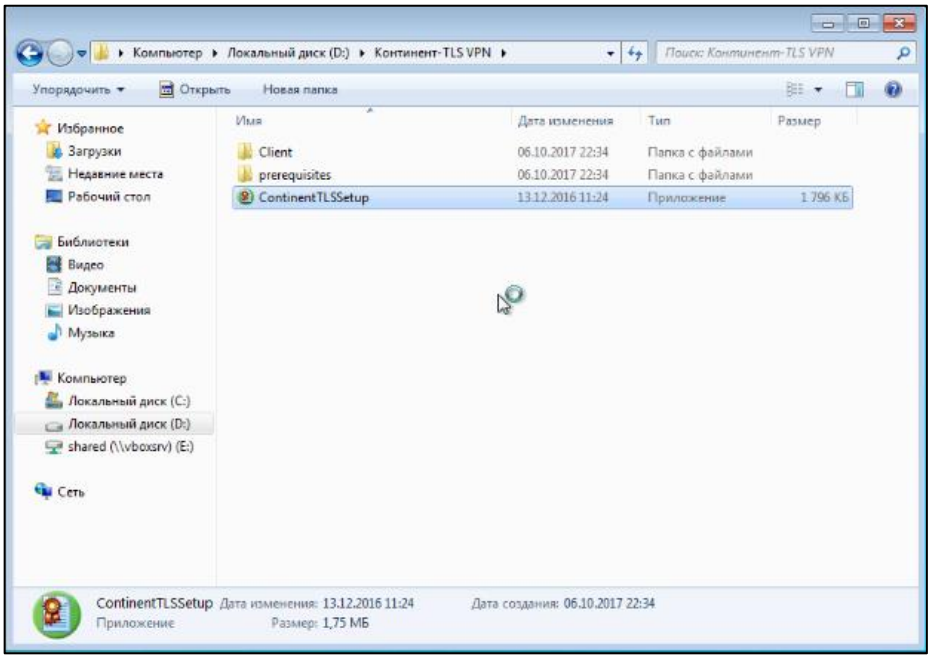

Рисунок 23 – Установочный файл «ContinentTLSSetup.exe»

Примечание – Из всех перечисленных компонентов обязательным для установки является «Континент TLS Клиент в исполнении КС1» (Рисунок 24).

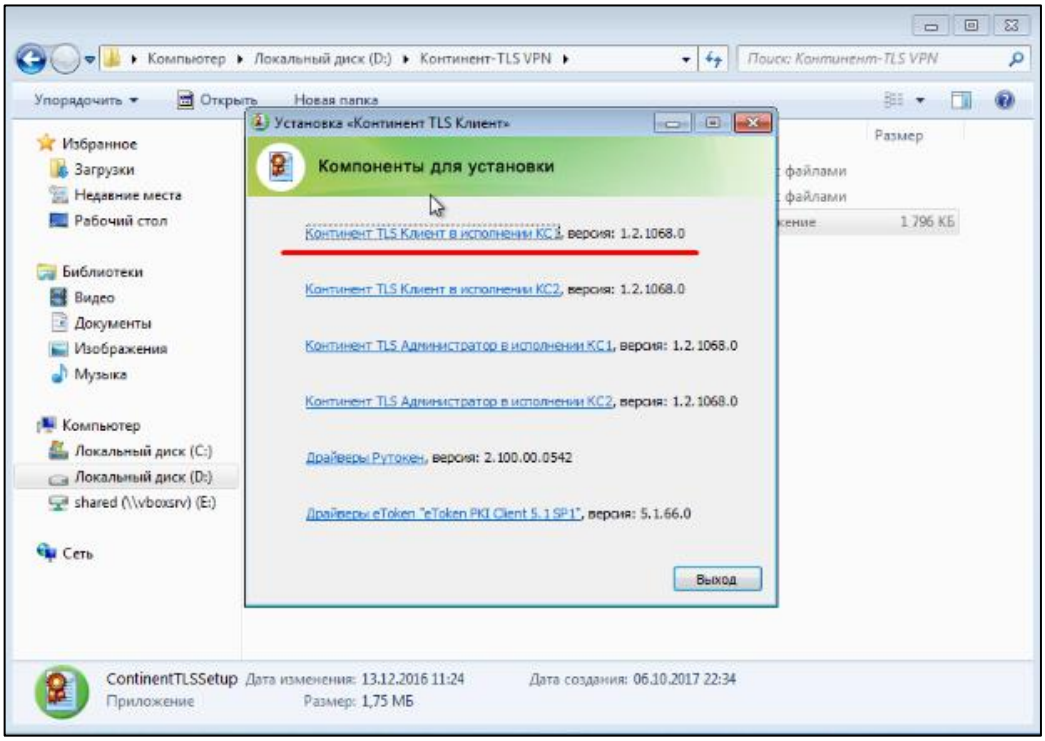

Рисунок 24 – Компонент «Континент TLS Клиент в исполнении КС1»

– выберите компонент «Континент TLS Клиент в исполнении КС1». На экране появится стартовое окно мастера установки компонента (Рисунок 25). Нажмите кнопку «Далее»;

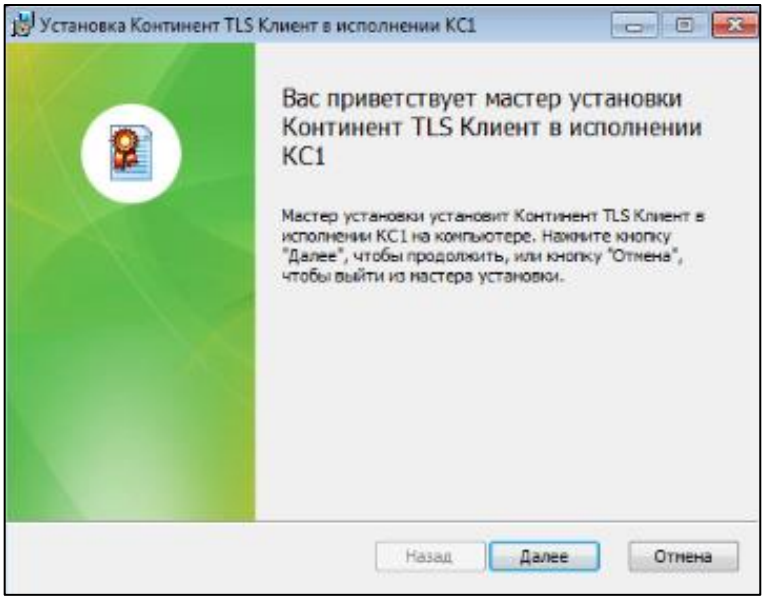

Рисунок 25 – Окно мастера установки компонента «Континент TLS Клиент в исполнении КС1»

– на экране появится окно лицензионного соглашения. Согласитесь с условиями лицензионного соглашения, установив «флажок» в поле «Я принимаю условия» и нажав кнопку «Далее» (Рисунок 26);

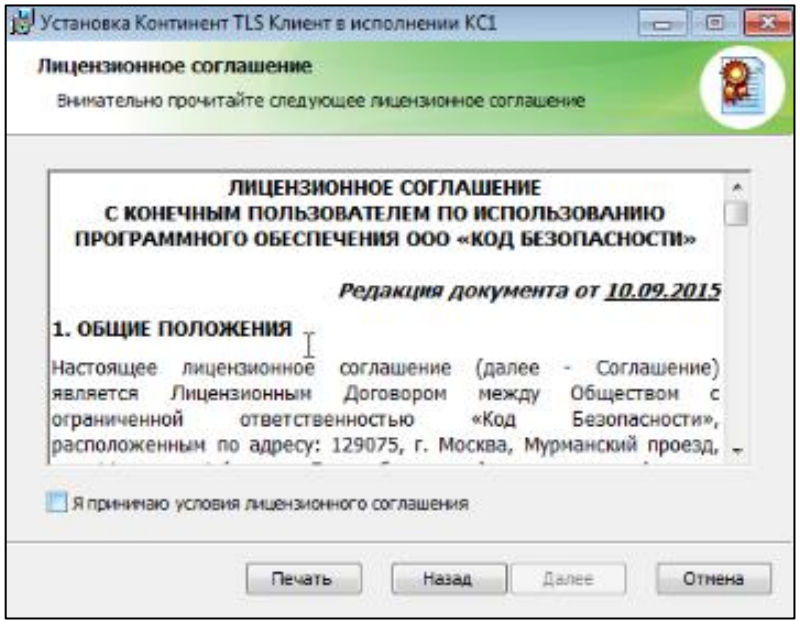

Рисунок 26 – Окно лицензионного соглашения

– 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». Нажмите кнопку «Далее» (Рисунок 27);

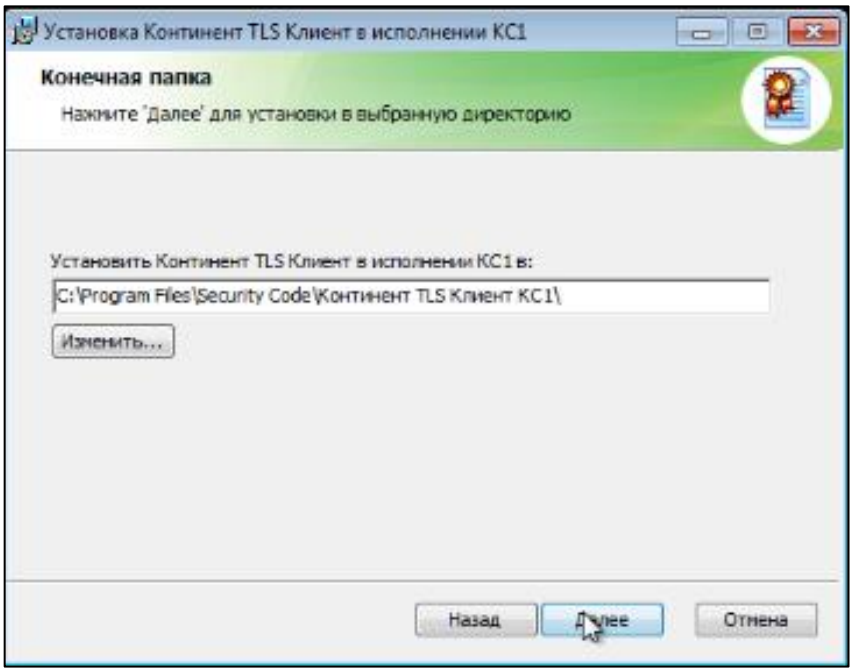

Рисунок 27 – Расположение каталога для разворачивания компонента «Континент TLS Клиент в исполнении КС1»

– в окне с информацией о готовности к установке нажмите кнопку «Установить» (Рисунок 28). Запустится процесс установки, который займет некоторое время;

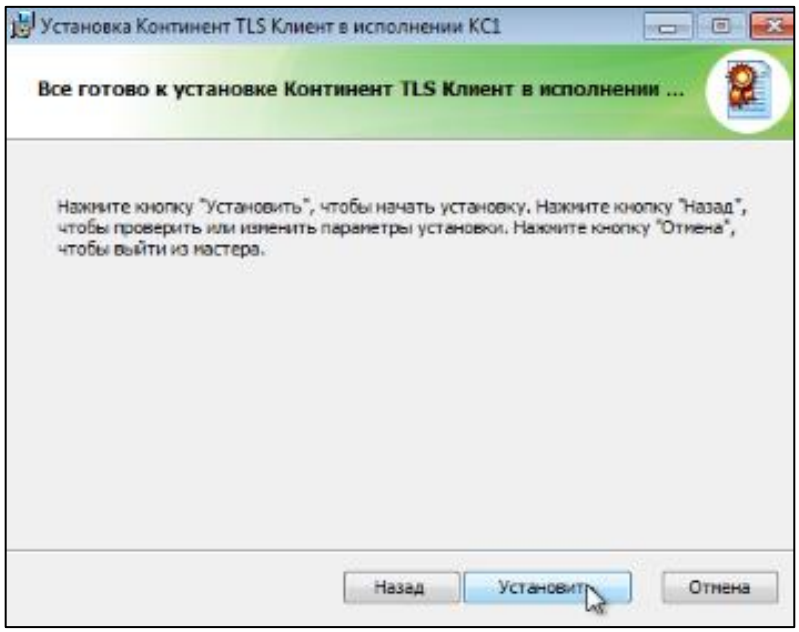

Рисунок 28 – Информация о готовности к установке компонента «Континент TLS Клиент в исполнении КС1»

– в окне с информацией о завершении установки нажмите кнопку «Готово» (Рисунок 29).

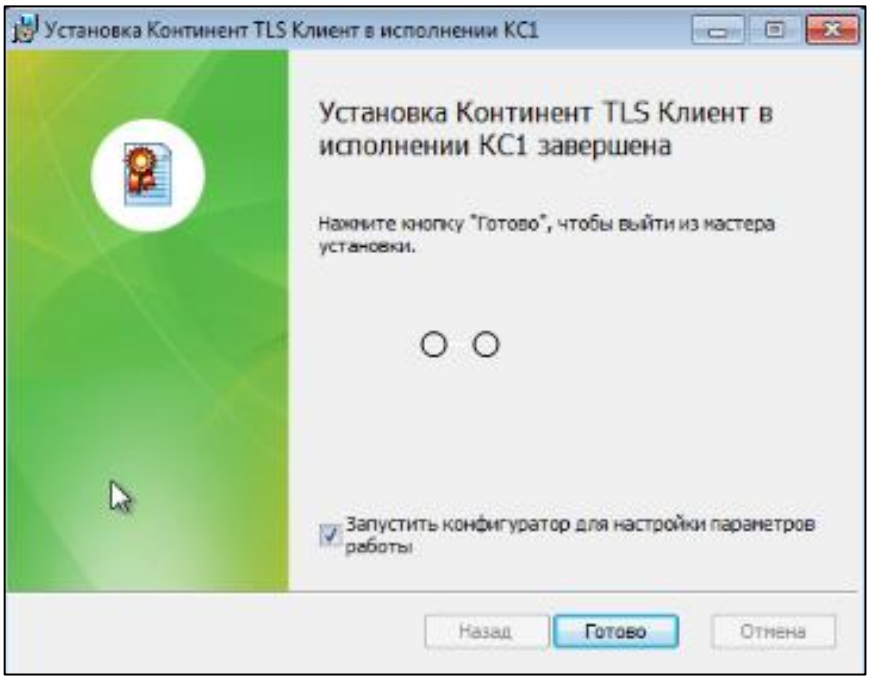

Рисунок 29 – Информация о завершении установки

– отобразится окно «Код Безопасности CSP». Нацельтесь на появившееся изображение мишени и нажмите на него левой кнопкой мыши (Рисунок 30);

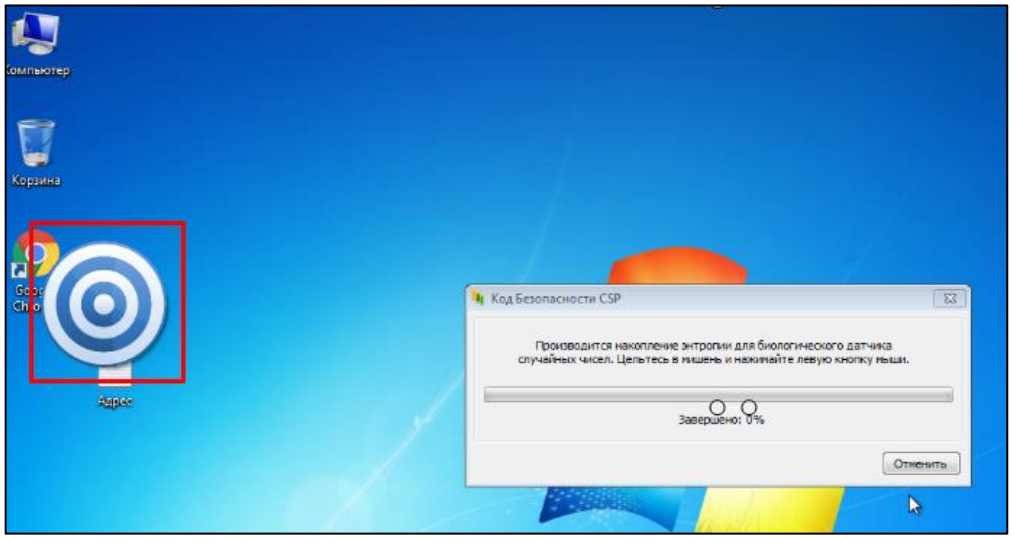

Рисунок 30 – Мишень

– в окне «Вектор успешно изменен» нажмите кнопку «ОК»;

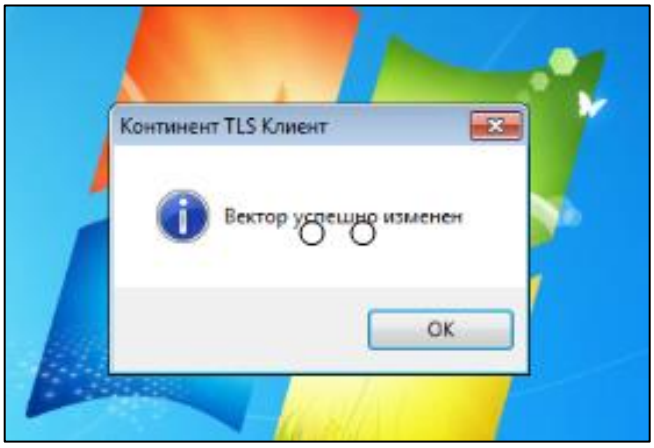

Рисунок 31 – Окно «Вектор успешно изменен»

Примечание – В случае возникновения ошибки при создании вектора энтропии, проигнорируйте ее и продолжите настройку в соответствии с настоящей инструкцией, наличие вектора не критично для подключения и корректной работы во ФГИС ЦС.

– откроется окно «Настройки Континент TLS Клиента КС1». Перейдите на вкладку «Настройки программы» (Рисунок 32);

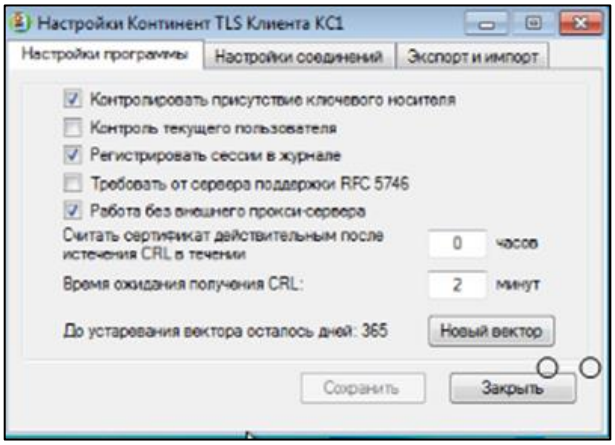

Рисунок 32 – Закладка «Настройки программы»

– убедитесь, что установлены «флажки» в полях следующих разрешений:
  – «Контролировать присутствие ключевого носителя»;
  – «Регистрировать сессии в журнале»;
  – «Работа без внешнего прокси-сервера» (в случае если прокси-сервер используется, данный «флажок» не должен быть установлен).
– перейдите на вкладку «Настройки соединений». Нажмите кнопку «Добавить соединение». В поле «Адрес/имя сервера» укажите значение «fgiscs-tls.gge.ru:8443», разрешите использовать туннель, установив «флажок» в поле «Туннель», и нажмите кнопку «Далее» (Рисунок 33);

Примечание – В имени сервера не должно быть опечаток, пробелов или прочих посторонних символов – оно должно строго соответствовать указанному выше значению.

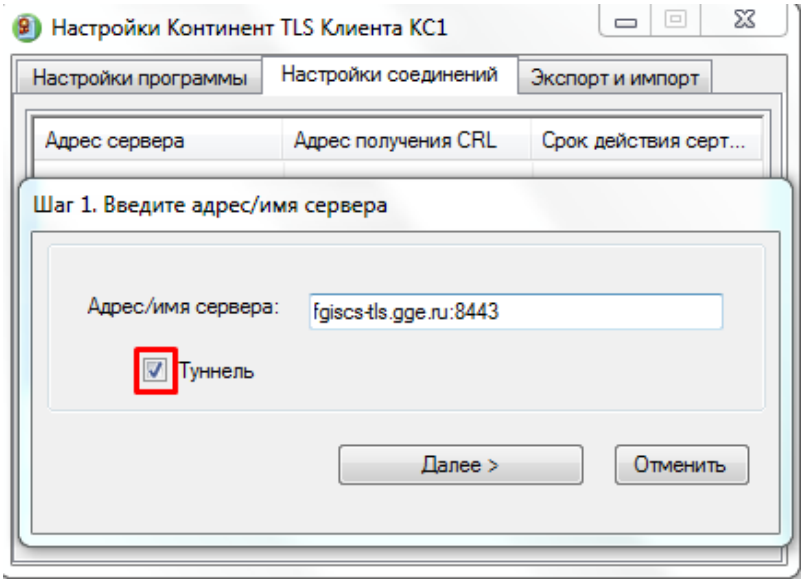

Рисунок 33 – Окно «Шаг 1. Введите адрес/имя сервера»

– в окне «Шаг 2. Укажите сертификат сервера» нажмите кнопку «Выбрать сертификат» (Рисунок 34);

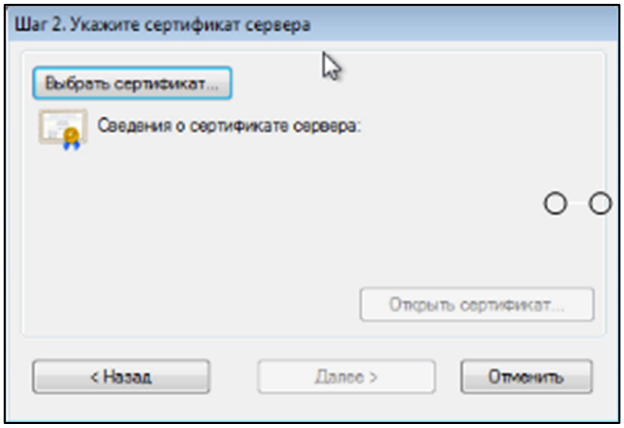

Рисунок 34 – Окно «Шаг 2. Укажите сертификат сервера»

– укажите Сертификат сервера для ПО «Континент TLS VPN», ранее полученный на Портале ФГИС ЦС в разделе «База знаний» в подразделе «Обучающие материалы» (https://fgiscs.minstroyrf.ru/#/educationalMaterial). Нажмите кнопку «Открыть» (Рисунок 35);

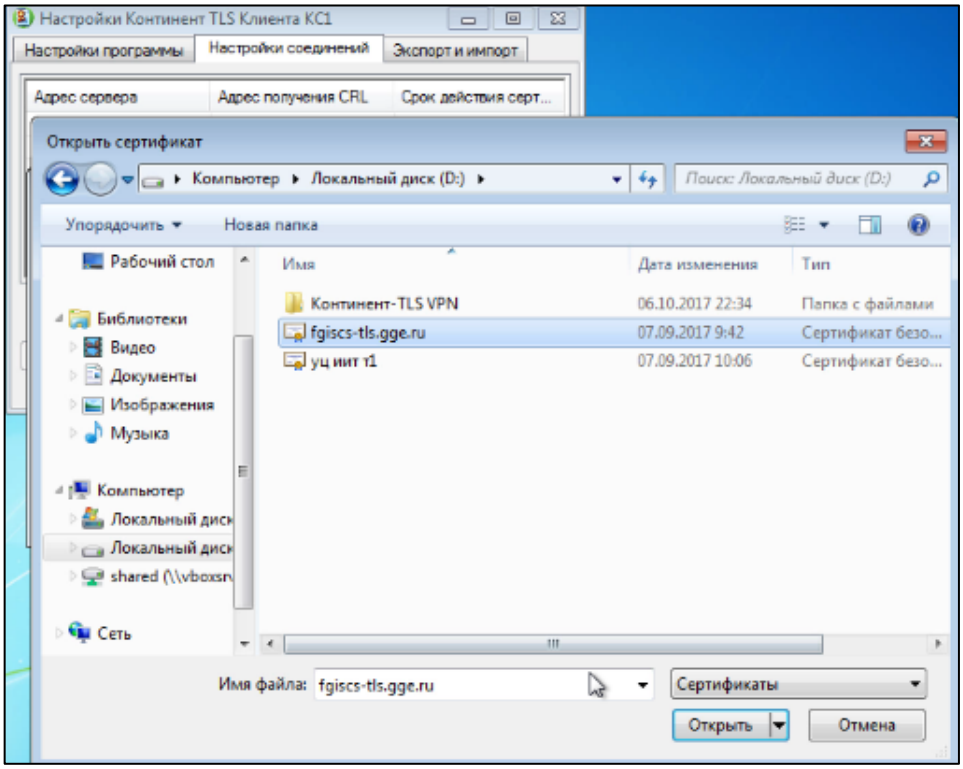

Рисунок 35 – Выбор сертификата

– нажмите кнопку «Открыть сертификат» (Рисунок 36);

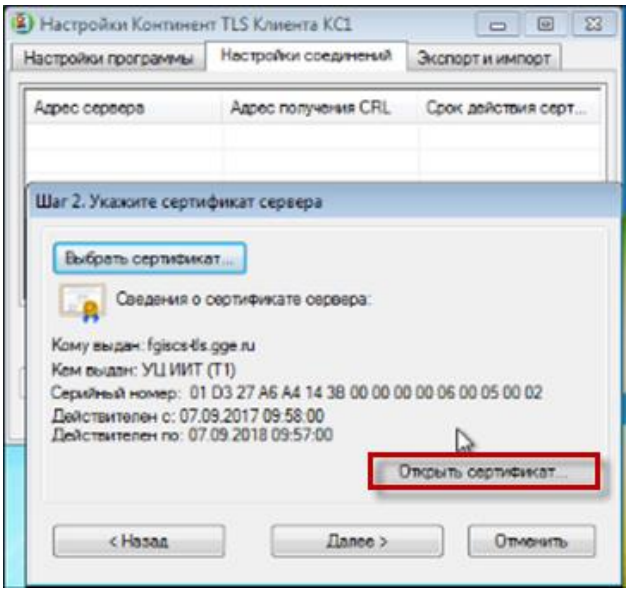

Рисунок 36 – Кнопка «Открыть сертификат»

– в открывшемся окне «Сертификат сервера» нажмите кнопку «Установить сертификат» (Рисунок 37);

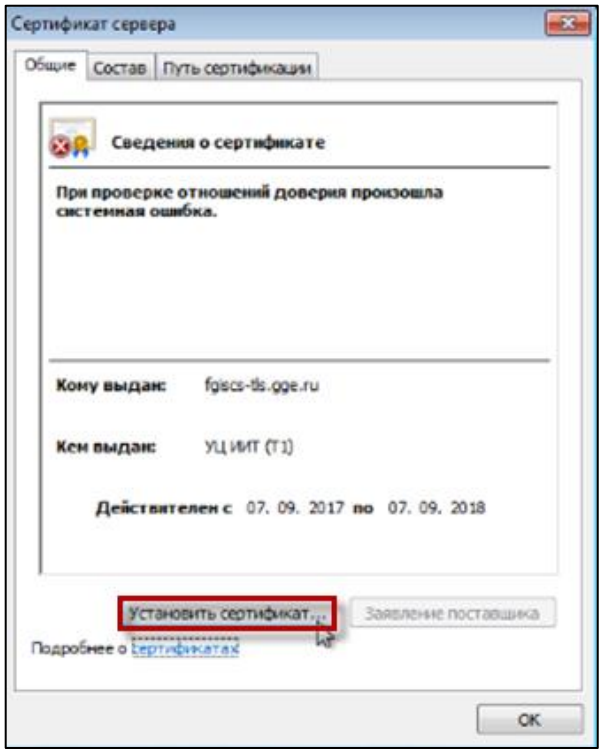

Рисунок 37 – Кнопка «Установить сертификат»

– в окне «Мастер импорта сертификатов» нажмите кнопку «Далее» (Рисунок 38);

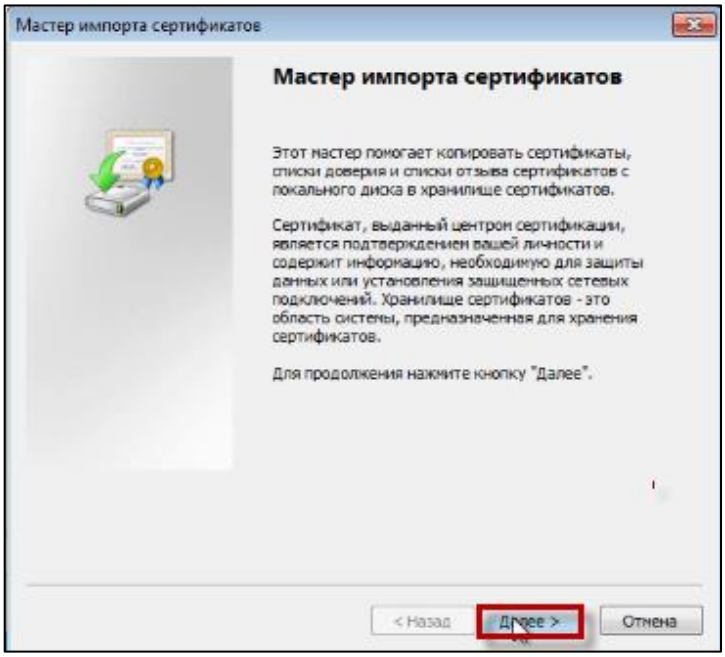

Рисунок 38 – Кнопка «Далее»

– установите переключатель на значение «Автоматически выбирать хранилище на основе типа сертификата», нажмите кнопку «Далее» (Рисунок 39);

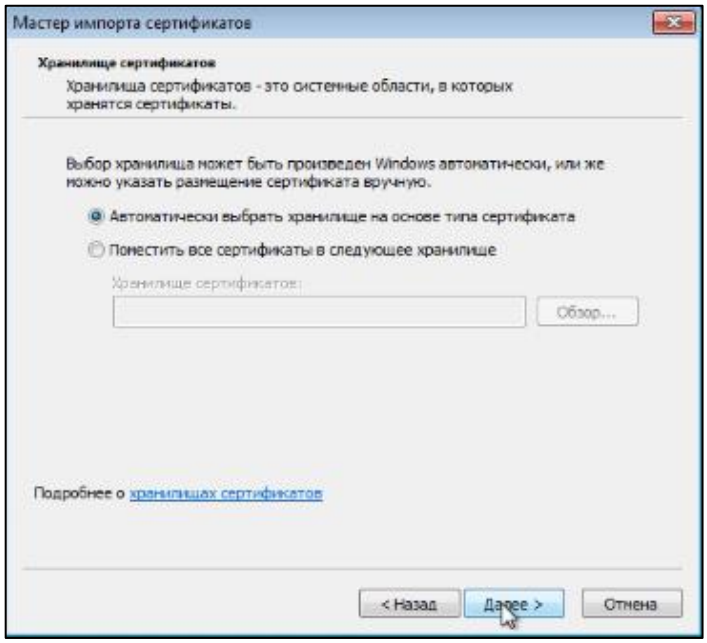

Рисунок 39 – Выбор параметра «Автоматически выбирать хранилище на основе типа сертификата»

– в окне «Завершение мастера импорта сертификатов» нажмите кнопку «Готово» (Рисунок 40);

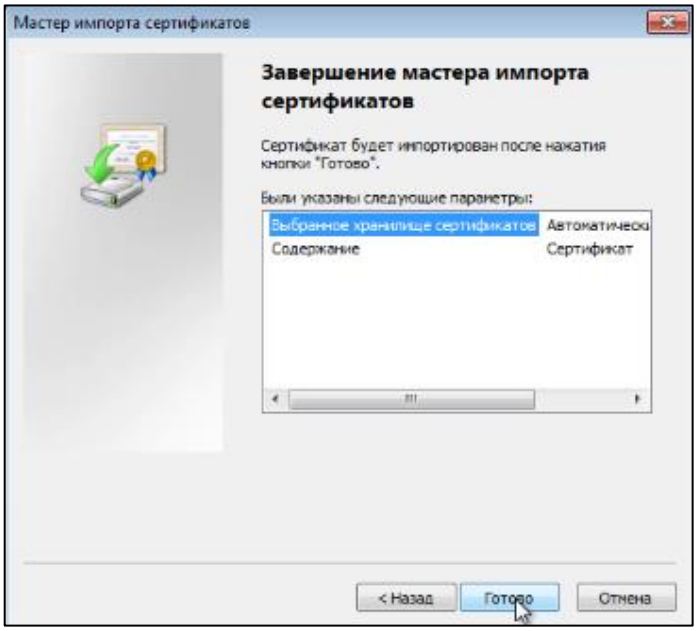

Рисунок 40 – Кнопка «Готово»

– в окне «Импорт успешно выполнен» нажмите кнопку «ОК» (Рисунок 41);

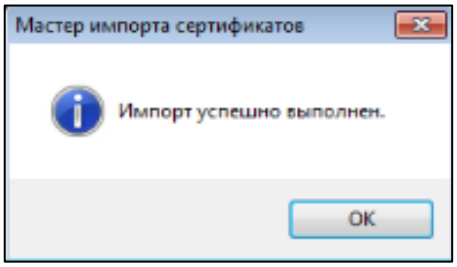

Рисунок 41 – Окно «Импорт успешно выполнен»

– нажмите кнопку «ОК» для закрытия окна «Сертификат сервера» (Рисунок 42);

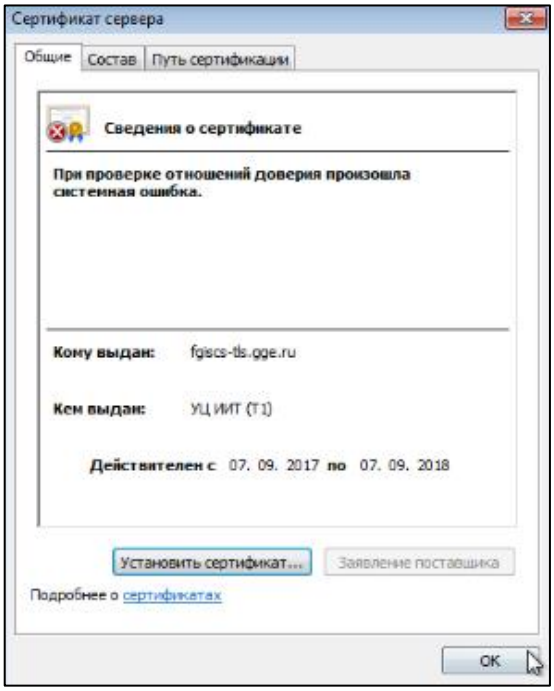

Рисунок 42 – Окно «Сертификат сервера»

– в окне «Шаг 2. Укажите сертификат сервера» нажмите кнопку «Далее» (Рисунок 43);

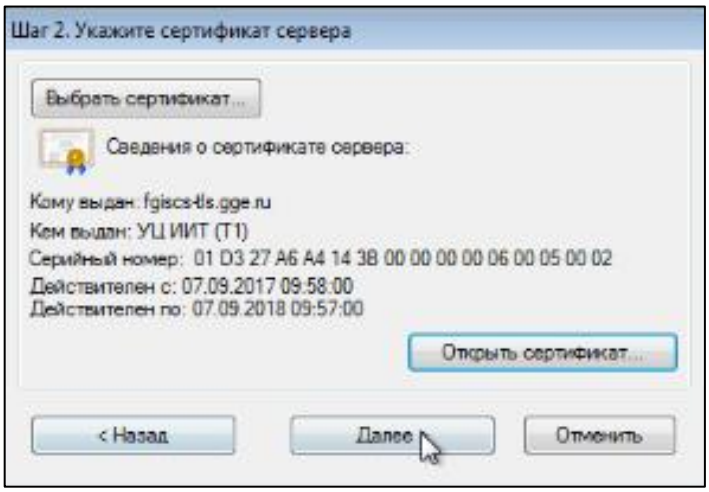

Рисунок 43 – Окно «Шаг 2. Укажите сертификат сервера»

– в окне «Шаг 3. Выбрать сертификат издателя» нажмите кнопку «Выбрать сертификат» (Рисунок 44);

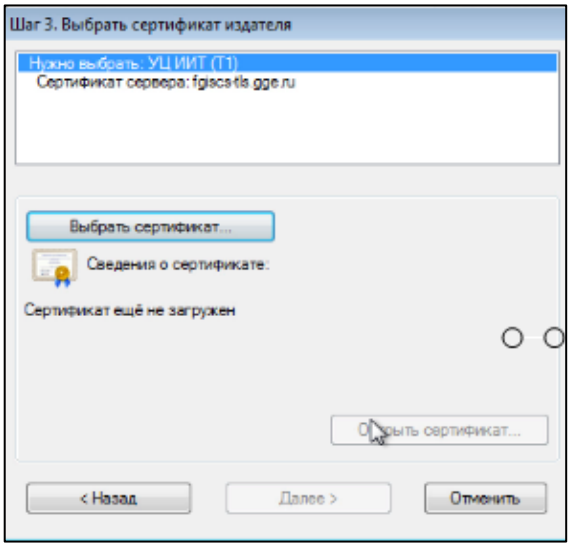

Рисунок 44 – Окно «Шаг 3. Выбрать сертификат издателя»

– укажите путь к сертификату «Сертификат Удостоверяющего Центра», загруженному с официального сайта https://fgiscs.minstroyrf.ru/#/educationalMaterial (Рисунок 45);

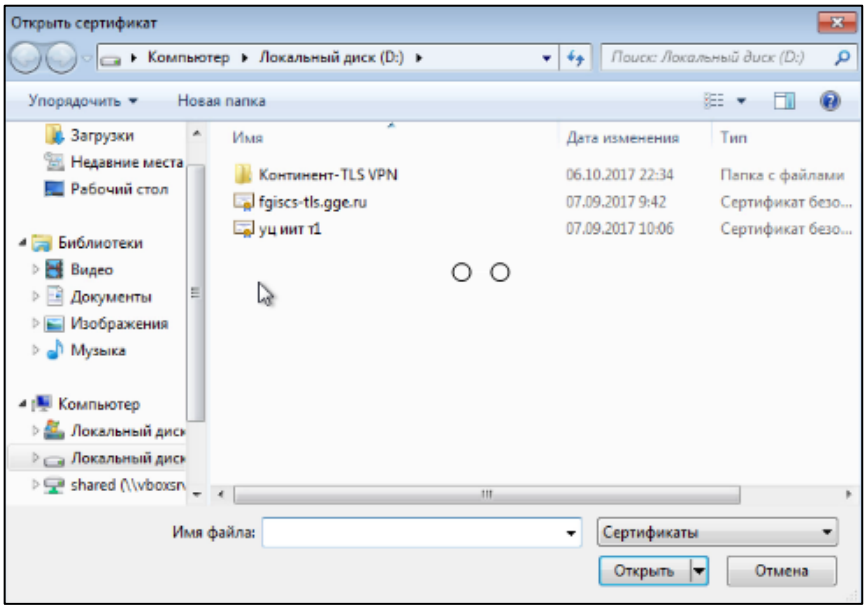

Рисунок 45 – Выбор сертификата

– выделите сертификат и нажмите кнопку «Открыть сертификат» (Рисунок 46);

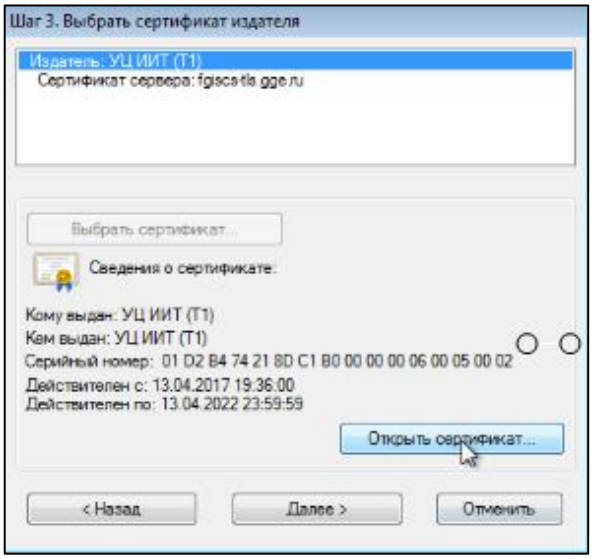

Рисунок 46 – Выбор сертификата

– в окне «Сертификат» нажмите кнопку «Установить сертификат» (Рисунок 47);

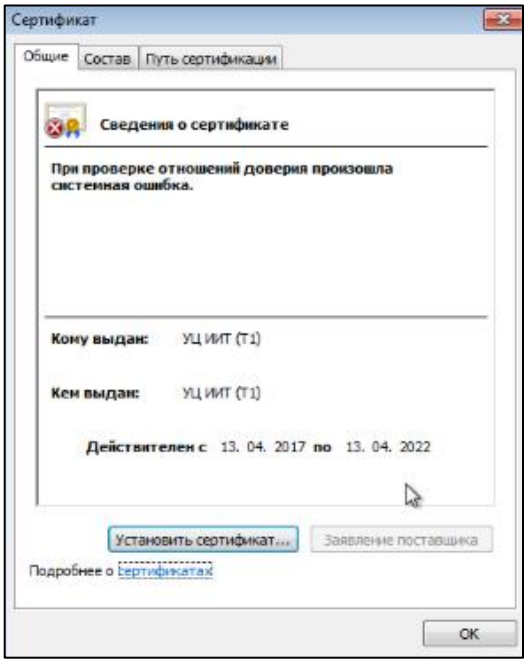

Рисунок 47 – Окно «Сертификат»

– в окне «Мастер импорта сертификатов» нажмите кнопку «Далее» (Рисунок 48);

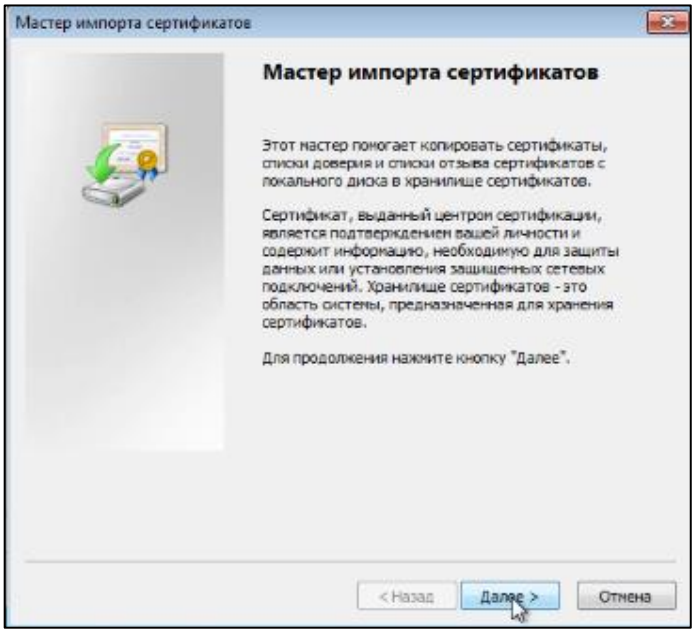

Рисунок 48 – Кнопка «Далее»

– установите переключатель на значение «Автоматически выбирать хранилище на основе типа сертификата», нажмите кнопку «Далее» (Рисунок 49);

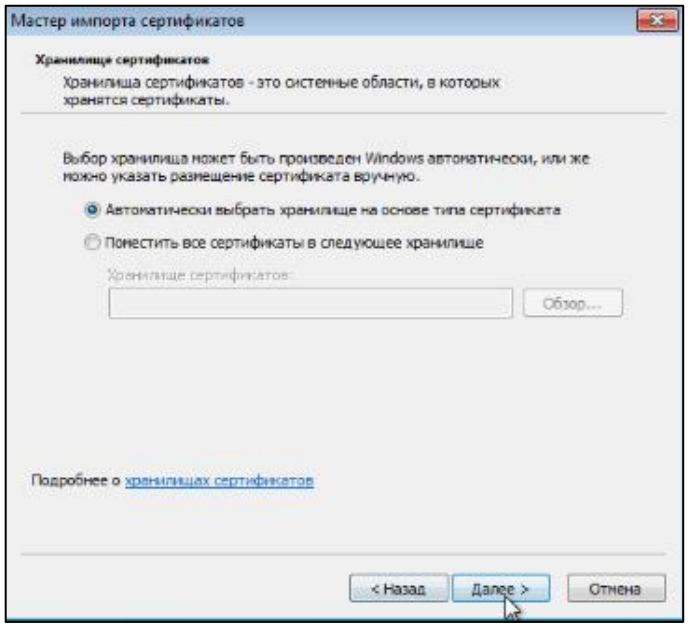

Рисунок 49 – Выбор параметра «Автоматически выбирать хранилище на основе типа сертификата»

– в окне «Завершение мастера импорта сертификатов» нажмите кнопку «Готово» (Рисунок 50);

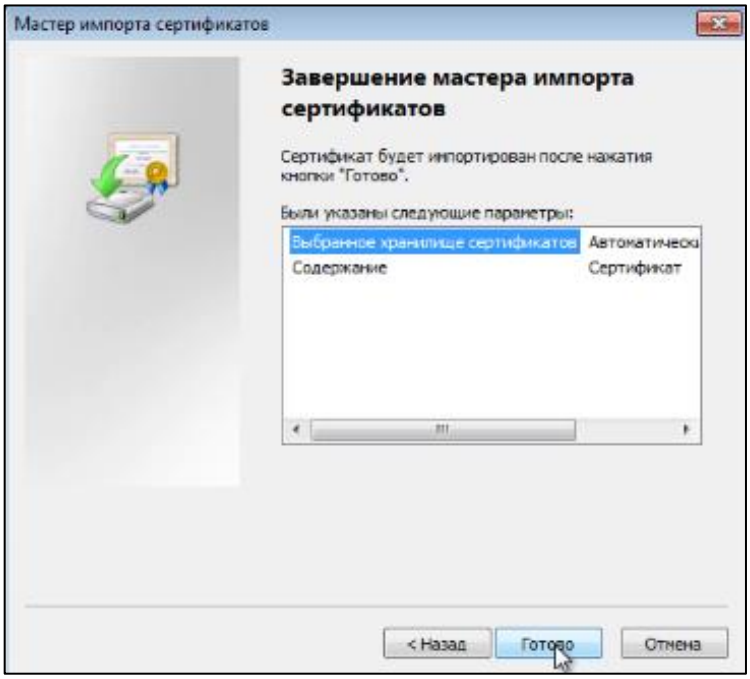

Рисунок 50 – Окно «Завершение мастера импорта сертификатов»

– в окне с сообщением «Импорт успешно выполнен» нажмите кнопку «ОК» (Рисунок 51);

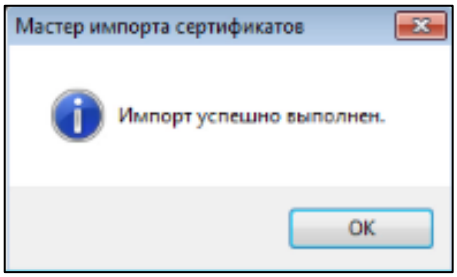

Рисунок 51 – Сообщение «Импорт успешно выполнен»

– в окне «Шаг 3. Выбрать сертификат издателя» нажмите кнопку «Далее» (Рисунок 52);

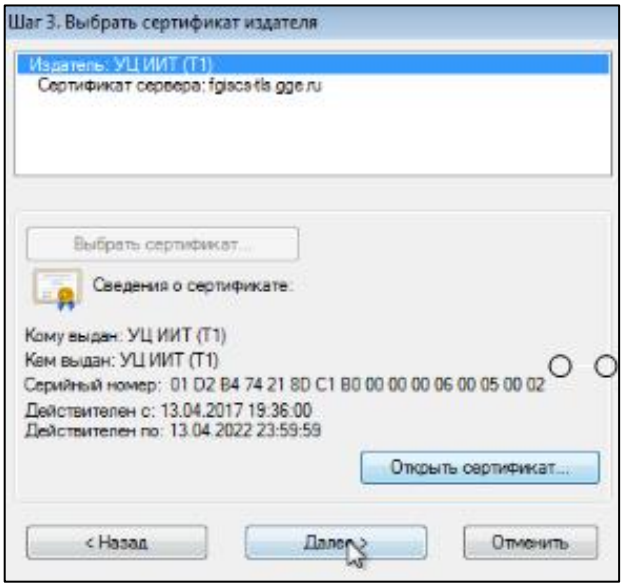

Рисунок 52 – Окно «Шаг 3. Выбрать сертификат издателя»

– откроется окно «Шаг 4. Укажите адрес получения CRL списка». Действия по настройке в данном окне выполнять не нужно, нажмите кнопку «Далее» (Рисунок 53);

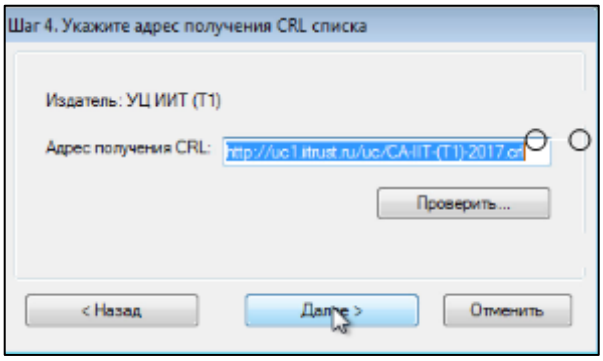

Рисунок 53 – Окно «Шаг 4. Укажите адрес получения CRL списка»

– в окне «Создание защищенного соединения завершено» нажмите кнопку «ОК» (Рисунок 54);

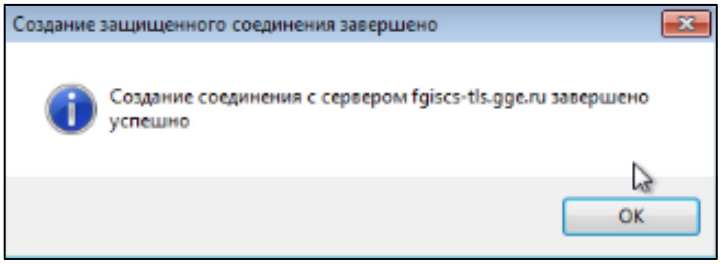

Рисунок 54 – Окно «Создание защищенного соединения завершено»

– в окне «Настройки Континент TLS Клиента КС1» нажмите кнопку «Сохранить» (Рисунок 55);

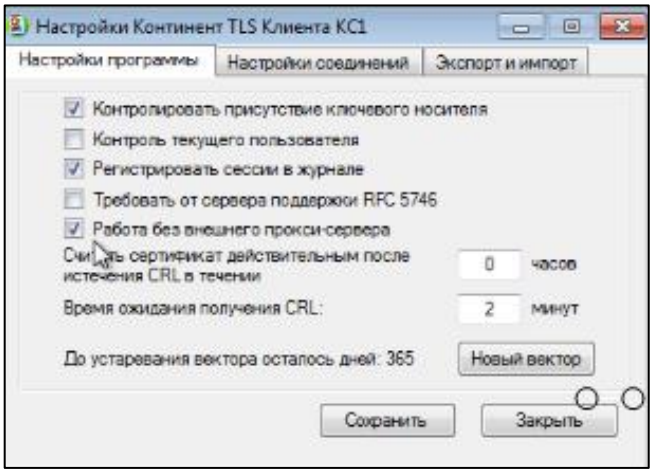

Рисунок 55 – Окно «Настройки Континент TLS Клиента КС1»

– откроется информационное окно с сообщением: «Адрес 127.0.0.1:8080 установлен как системный прокси-сервер», если внешний прокси-сервер не используется, или сообщение «Необходимо задать корректные системные настройки прокси-сервера» в случае, если таковой используется (Рисунок 56, Рисунок 57);

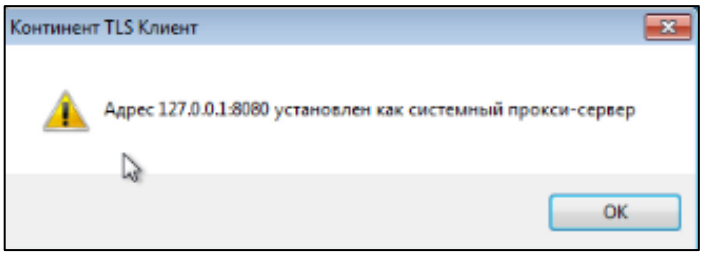

Рисунок 56 – Информационное сообщение (внешний прокси-сервер не используется)

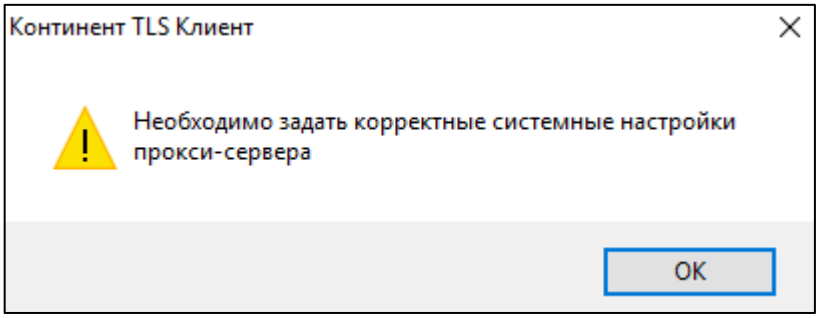

Рисунок 57 – Информационное сообщение (внешний прокси-сервер используется)

– нажмите кнопку «ОК», отобразится информационное окно с сообщением: «Настройки программы успешно сохранены» (Рисунок 58);

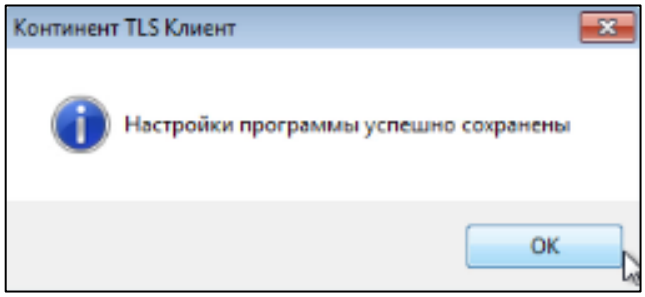

Рисунок 58 – Информационное сообщение

– проверьте настройки прокси-сервера:
  – нажмите кнопку «Пуск»;
  – нажмите кнопку «Панель управления»;
  – выберите раздел «Свойства web-браузера». На экране появится окно «Свойства: Интернет» (Рисунок 59);

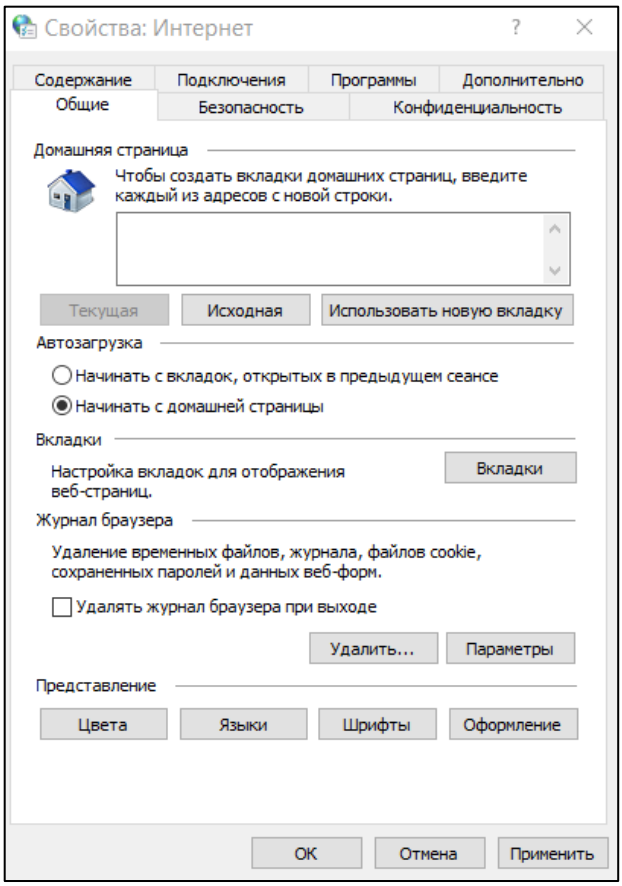

Рисунок 59 – Окно «Свойства: Интернет»

  – перейдите на вкладку «Подключения», затем нажмите кнопку «Настройка сети» (Рисунок 60);
  – убедитесь, что в поле настройки «Использовать прокси-сервер для локальных подключений» установлен «флажок»;

– проверьте значения: в поле «Адрес» должно быть установлено значение «127.0.0.1», в поле «Порт» – «8080» в случае, если в организации не используется прокси-сервер, или сетевой адрес и порт, если таковой используется;

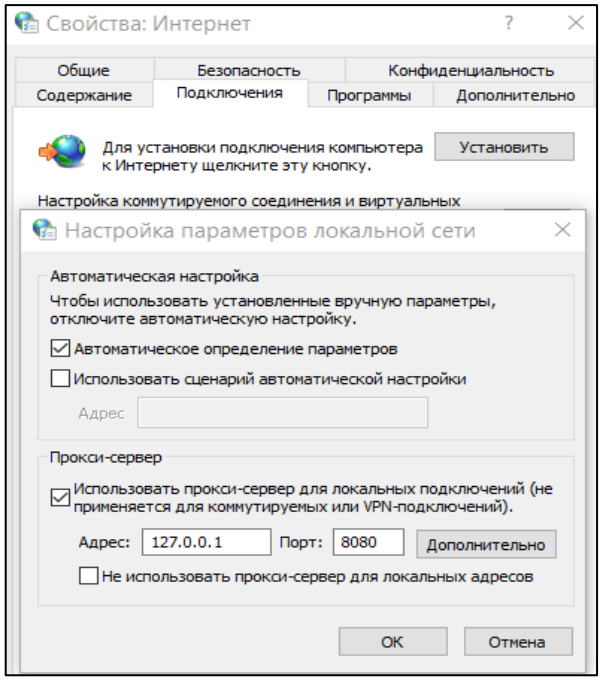

Рисунок 60 – Настройки прокси-сервера

– дважды последовательно нажмите кнопки «ОК».

Для создания защищенного соединения с сервером выполните следующие действия:

– откройте web-браузер, например, «Google Chrome»;
– введите адрес сервера https://fgiscs-tls.gge.ru:8443 в адресной строке web-браузера и нажмите клавишу «Enter»;
– убедитесь, что внешний носитель, содержащий пользовательскую электронную подпись, предварительно полученную в аккредитованном Удостоверяющем центре, подключен к компьютеру;
– на экране откроется окно «Континент TLS VPN» (Рисунок 61), выберите хранилище, в котором хранится криптоконтейнер;

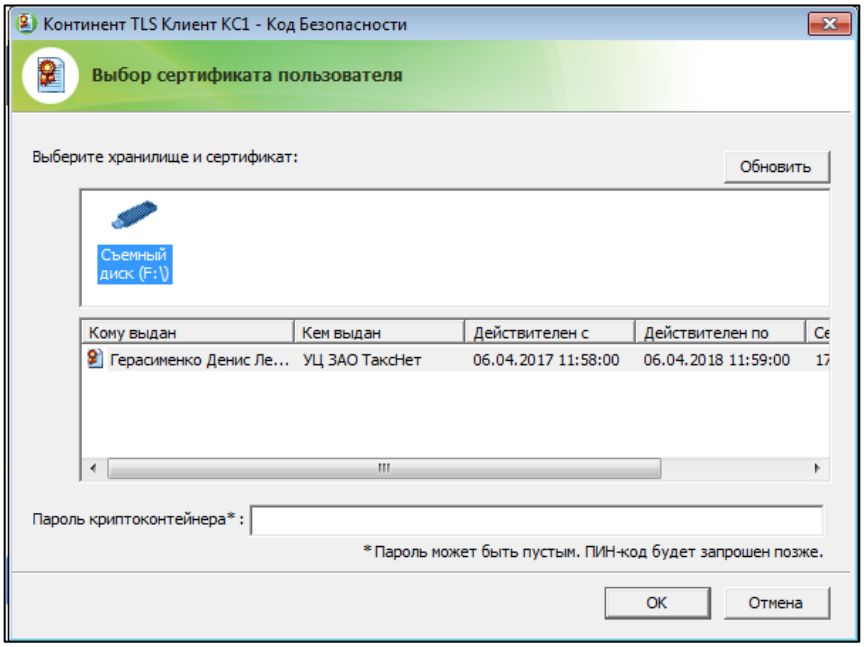

Рисунок 61 – Окно «Континент TLS VPN» для выбора хранилища

– выберите действующий сертификат (Рисунок 62);

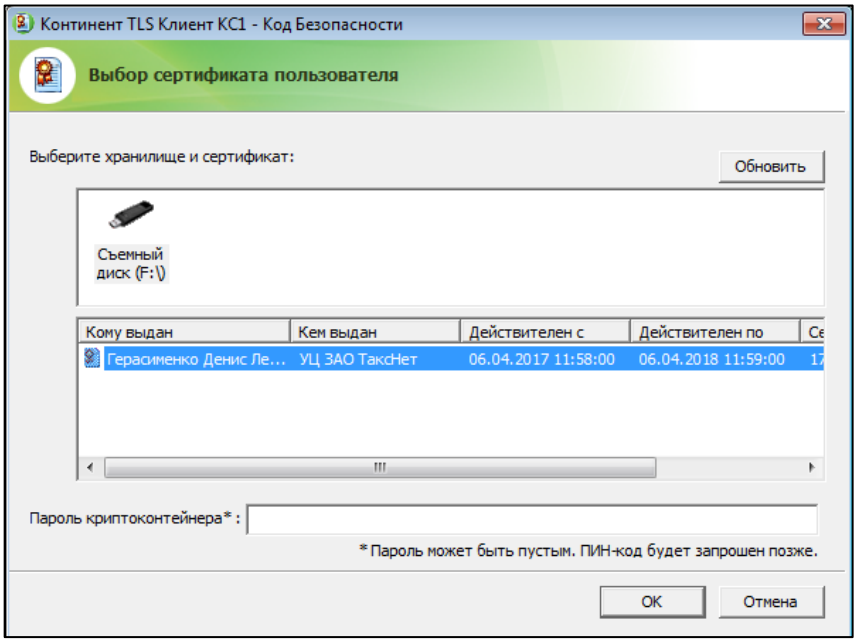

Рисунок 62 – Окно «Континент TLS VPN» выбора действующего сертификата

– введите пароль криптоконтейнера (если такой существует), полученный в комплекте УКЭП (Рисунок 63), и нажмите кнопку «ОК».

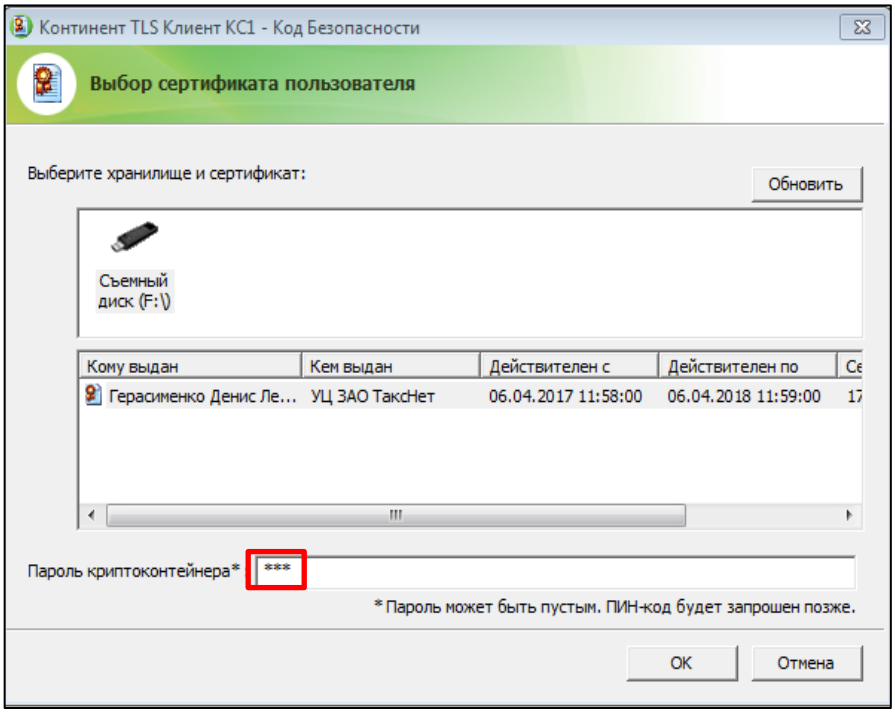

Рисунок 63 – Окно «Континент TLS VPN» с введенным паролем криптоконтейнера

Обратите внимание, что после нажатия кнопки «ОК» пиктограмма программного обеспечения «Континент TLS VPN» (Рисунок 64), размещенная в правом нижнем углу панели рабочего стола, изменит свой цвет с красного («не подключен») на зеленый («подключен») (Рисунок 65).

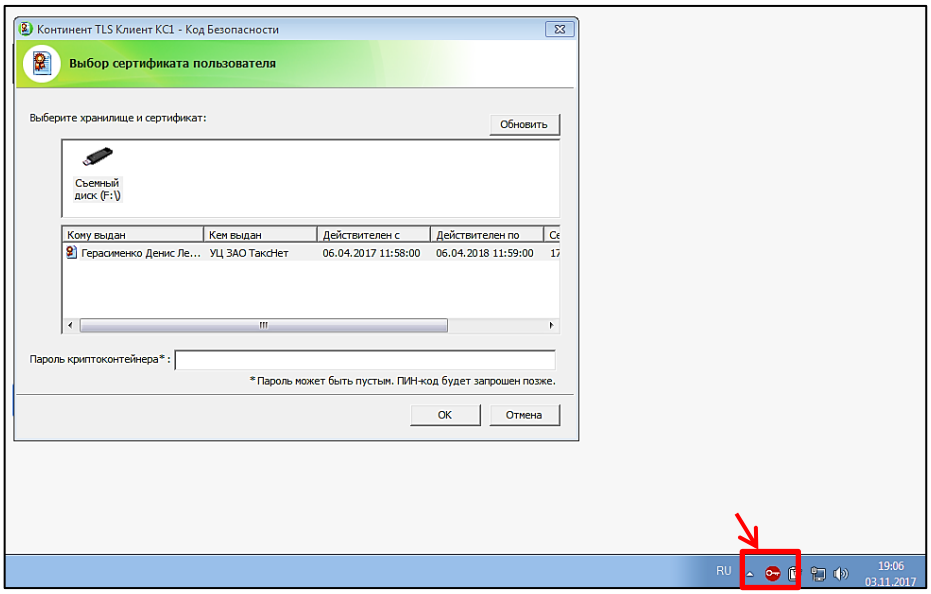

Рисунок 64 – Окно рабочего стола, красная пиктограмма «Континент TLS VPN»

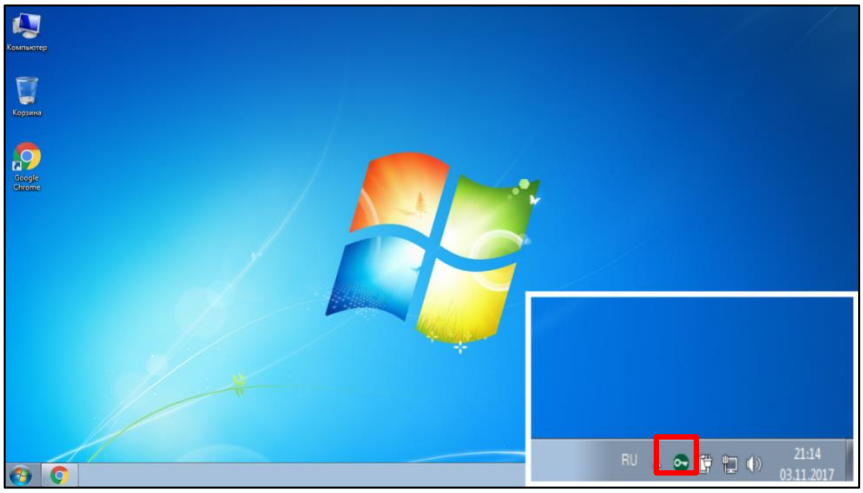

Рисунок 65 – Окно рабочего стола, зеленая пиктограмма «Континент TLS VPN»

На экране появится страница с сообщением «Ваше подключение не защищено» (Рисунок 66). Выполните необходимые действия, чтобы обеспечить переход на Портал ФГИС ЦС и дальнейшую работу с Порталом ФГИС ЦС через защищенное соединение, для этого выполните следующие действия:

– нажмите кнопку «Дополнительные» (Рисунок 66);

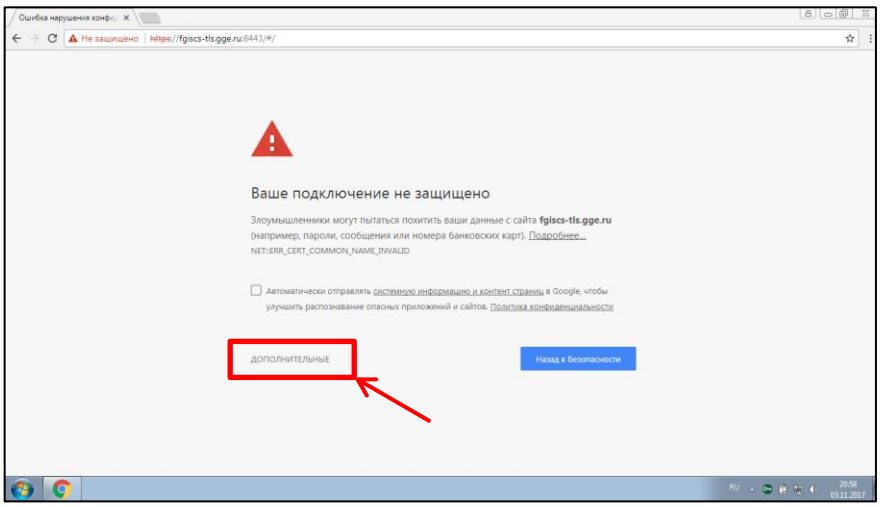

Рисунок 66 – Окно web-браузера «Google Chrome» для перехода на Портал ФГИС ЦС

– далее нажмите на ссылку «Перейти на сайт fgiscs-tls.gge.ru» (Рисунок 67);

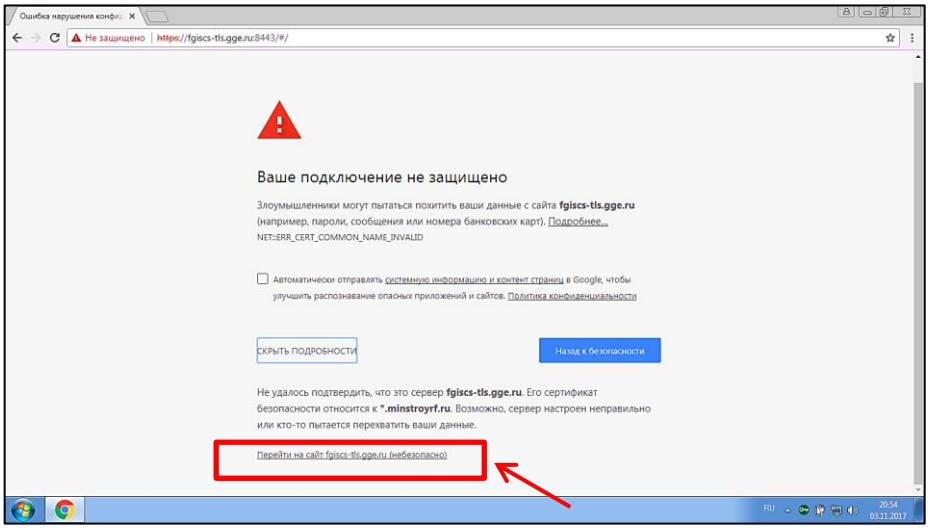

Рисунок 67 – Окно для перехода на Портал ФГИС ЦС

– выполните вход в личный кабинет ФГИС ЦС (см. п. 6).

Установка и настройка ПО «Континент TLS VPN» завершена.

6 Вход в личный кабинет ФГИС ЦС

Для входа в личный кабинет ФГИС ЦС выполните следующие шаги:

- откройте web-браузер, например, «Google Chrome»;
- установите защищенное соединение, перейдя по ссылке https://fgiscs-tls.gge.ru:8443 и выбрав сертификат пользователя (см. п. 5 о создании защищенного соединения);
- перейдите на Портал ФГИС ЦС по ссылке: https://fgiscs.minstroyrf.ru/;
- нажмите кнопку «Личный кабинет», отображаемую в виде ссылки (Рисунок 68);
- откроется страница портала ЕСИА для авторизации в личном кабинете ФГИС ЦС.

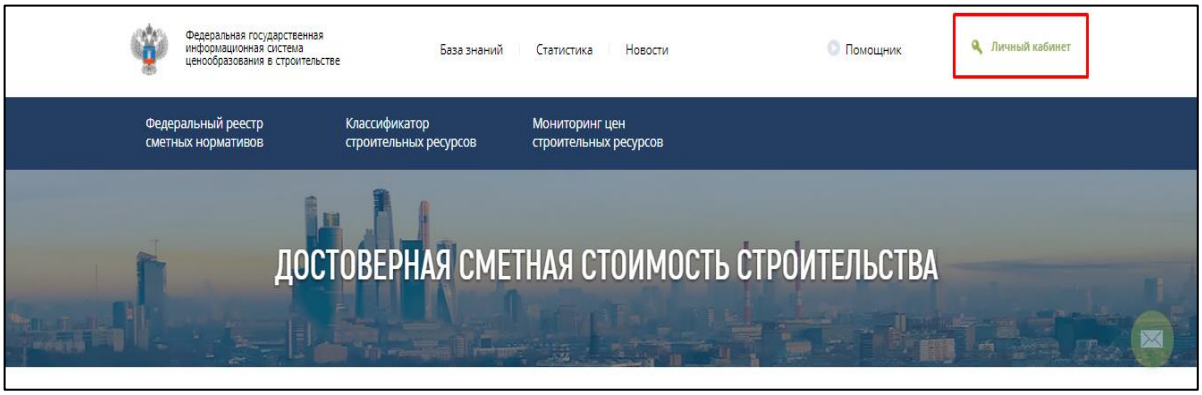

Рисунок 68 – Кнопка «Личный кабинет»

7 Часто задаваемые вопросы, ошибки и способы их устранения

7.1 Базовые требования

Вопрос

Какое ПО необходимо приобрести для работы во ФГИС ЦС?

Были закуплены ПО «Jinn-Client» и «Континент TLS VPN», нужно ли покупать что-либо еще?

Ответ

Для полноценной работы в закрытой части портала ФГИС ЦС (подключение по ссылке https://fgiscs-tls.gge.ru:8443) на АРМ пользователя должны быть установлены следующие СКЗИ:

– ПО «Jinn-Client» версия 1.0;

– ПО «Континент TLS VPN» версия 1.2.

Также пользователь должен обладать УКЭП, полученной в аккредитованном Удостоверяющем центре. Перечень аккредитованных Удостоверяющих центров доступен по ссылке: http://e-trust.gosuslugi.ru/CA.

7.2 Информационное письмо на сайте

Вопрос

При входе в личный кабинет появляется информационное сообщение (Рисунок 69).

Ответ

Подключение к закрытой части ФГИС ЦС по защищенному каналу происходит по ссылке https://fgiscs-tls.gge.ru:8443. Пожалуйста, проверьте, осуществляется ли подключение. Успешное подключение свидетельствует о корректной настройке ПО «Континент TLS VPN». Дополнительную информацию по работе с порталом можно найти по ссылке https://fgiscs.minstroyrf.ru/#/Knowledges или написав обращение с помощью формы на сайте https://fgiscs.minstroyrf.ru (пиктограмма  справа). Обратите внимание, что аутентификация в личном кабинете https://fgiscs.minstroyrf.ru происходит при успешно установленном соединении с сервером https://fgiscs-tls.gge.ru:8443.

Если подключение к https://fgiscs-tls.gge.ru:8443 не выполняется, перейдите к п. 7.7.

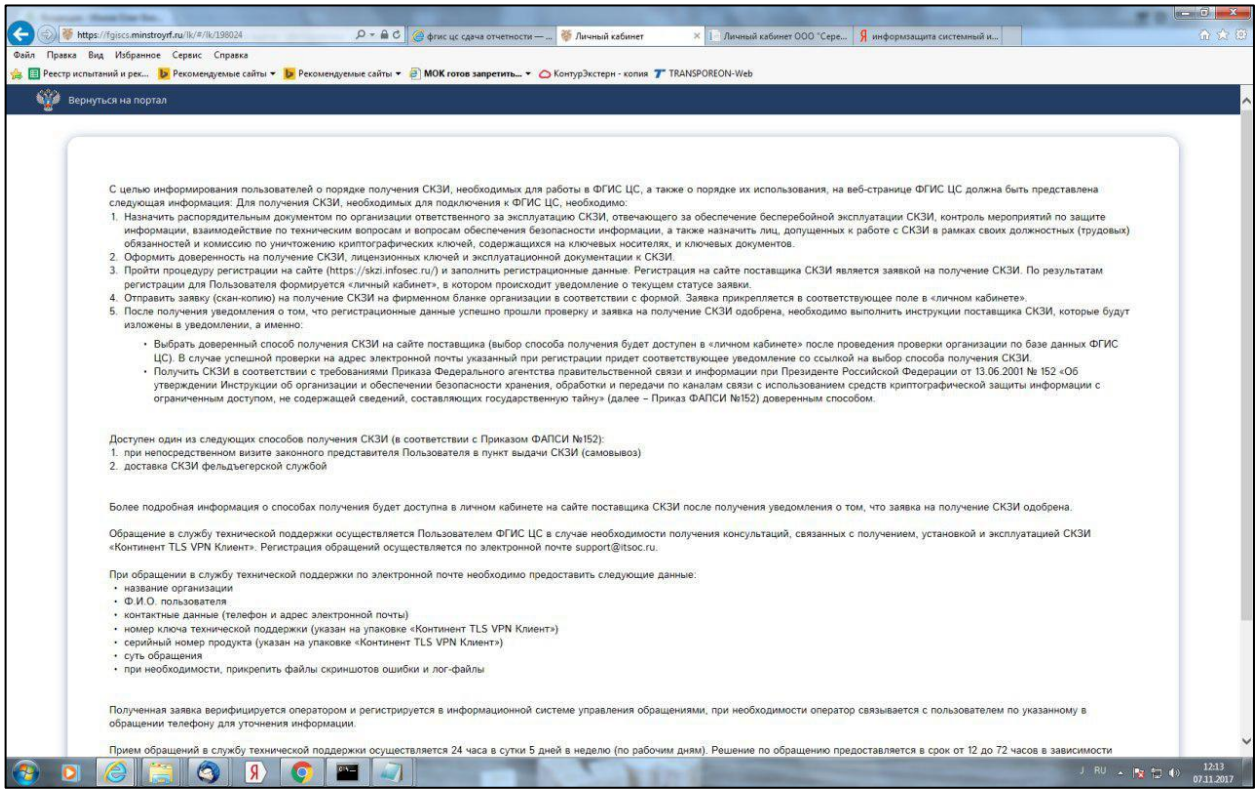

Рисунок 69 – Информационное сообщение

7.3 ПО «Континент TLS VPN» версии 2.0

Вопрос

Любой вопрос, связанный с ПО «Континент TLS VPN» версии 2.0.

Ответ

Временная версия 2.0 больше не распространяется и для подключения к ФГИС ЦС необходимо получить версию 1.2 в рамках процедур, предлагаемых на портале skzi.infosec.ru или приобрести сертифицированный дистрибутив версии 1.2 у любого партнера «Кода Безопасности».

7.4 ПО «Континент TLS VPN»/ ПО «Jinn-Client» не видит ключ

Вопрос

При входе в личный кабинет возникает окно выбора сертификата ПО «Континент TLS VPN», но окно пустое. Аналогично, при подписи документа возникает окно выбора сертификата ПО «Jinn-Client», но окно пустое (Рисунок 70).

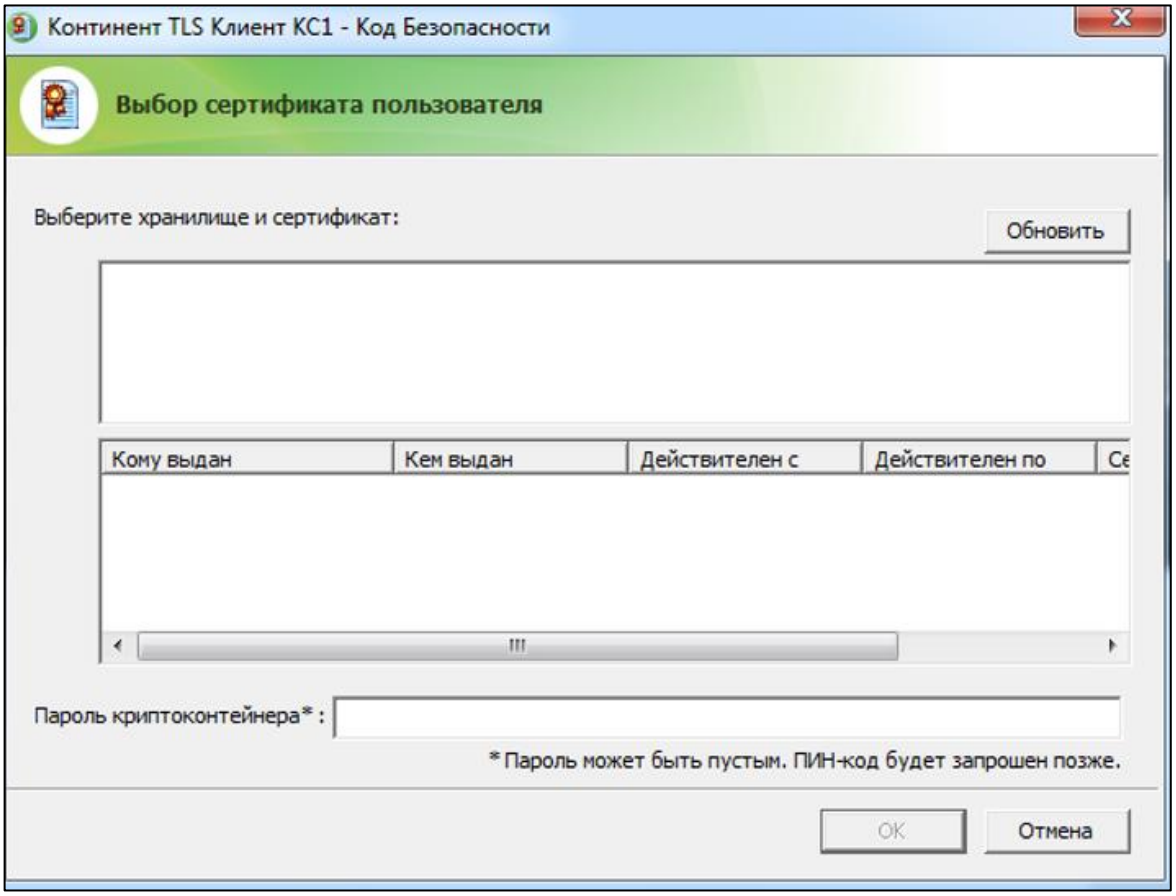

Рисунок 70 – Выбор сертификата пользователя (пустое окно)

Ответ

Поддерживаются только следующие носители ключевой информации сертификата пользователя (дискеты не поддерживаются):

– USB флеш-накопитель;

– Rutoken S (Rutoken Lite, Rutoken ЭЦП не поддерживаются);

– eToken Pro;

– eToken PRO (Java).

Перенесите закрытый ключ на поддерживаемый тип носителя. Для этого в КриптоПро CSP перейдите на вкладку «Сервис», нажмите кнопку «Скопировать», следуйте указаниям мастера копирования.

При использовании Rutoken S установите соответствующий драйвер: https://www.rutoken.ru/support/download/drivers-for-windows/.

При Использовании eToken установите набор драйверов (https://www.aladdin-rd.ru/support/downloads/38524/ или https://www.aladdin-rd.ru/support/downloads/26037/) и единый клиент «JaCarta» (https://www.aladdin- rd.ru/support/downloads/43987/).

7.5 Запрос на сертификат

Вопрос

Был сформирован запрос на сертификат, каковы дальнейшие действия?

Ответ

Направьте запрос в любой аккредитованный удостоверяющий центр. Список данных Удостоверяющих центров можно найти по ссылке http://e-trust.gosuslugi.ru/CA

Уже имеющуюся УКЭП можно использовать без необходимости формировать запрос на сертификат.

7.6 400 Bad Request

Вопрос

При подключении к https://fgiscs-tls.gge.ru:8443 появляется сообщение об ошибке «400 Bad Request. The plain HTTP request was sent to HTTPS port» (Рисунок 71).

Рисунок 71 – Ошибка

Ответ

Данная ошибка возникает при подключении по протоколу http. Пожалуйста, перезапустите web-браузер и перейдите по ссылке https://fgiscs-tls.gge.ru:8443 (протокол https).

Если подключение не выполняется успешно, перейдите к п. 7.7.

7.7 Не удается получить доступ к сайту

Вопрос

Установлено ПО «Jinn-Client» и «Континент TLS VPN», при переходе по ссылке https://fgiscs.tls-gge.ru:8443 в окне web-браузера отображается сообщение: «Не удается получить доступ к сайту», или «Невозможно отобразить страницу», или «Соединение было сброшено» (Рисунок 72).

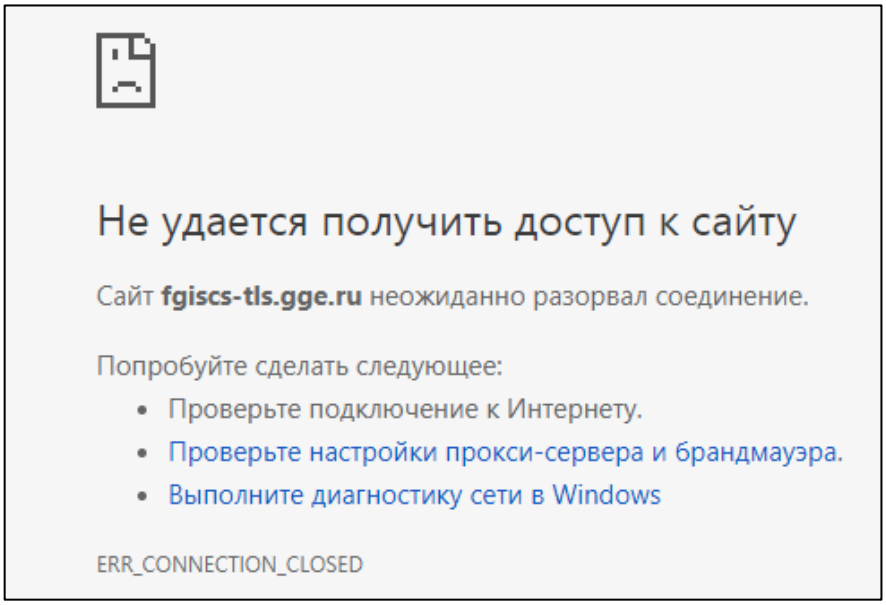

Рисунок 72 – Сообщение в окне web-браузера

Ответ

Ниже приведен перечень возможных причин возникновения данной ошибки. Пожалуйста, убедитесь, что все условия выполняются на АРМ пользователя:

- наличие сетевого доступа. Для проверки наличия сетевого доступа выполните в командной строке команду «telnet fgiscs-tls.gge.ru 8443» в командной строке. (Предварительно установите клиент «Telnet» см. п. 5.1). Признаком успешного выполнения команды является наличие мигающего курсора в командной строке. Если команда не выполняется, обратитесь к системному администратору для разрешения сетевого доступа от АРМ пользователя до «fgiscs-tls.gge.ru» по портам tcp 80, tcp 443, tcp 8443;
- отсутствие блокировок антивирусного ПО. Некоторые программы обнаружения вредоносного ПО могут блокировать трафик или работу службы «ContinentTLS». Пожалуйста, обратитесь к системному администратору для проверки, не блокируется ли трафик до «fgiscs-tls.gge.ru» по портам tcp 8443, 443, 80 и работа службы «ContinentTLS»;
- сертификат субъекта выдан аккредитованным Удостоверяющим центром. Перечень аккредитованных Удостоверяющих центров доступен по ссылке: http://e-trust.gosuslugi.ru/CA;
- корректные настройки ПО «Континент TLS VPN». Если окно выбора сертификата пользователя появляется, а ошибка возникает после выбора, настройки соединения верны. Если окно выбора сертификата пользователя не появляется, это

свидетельствует о некорректной настройке ПО «Континент TLS VPN»: необходимо проверить настройку в соответствии с п. 5 настоящей инструкции. Возможно, допущена опечатка в адресе сервера, либо не установлен «флажок» в поле «Туннель», либо выбраны неверные сертификаты.

Если все условия выполняются, пришлите, пожалуйста, скриншот ошибки и следующую информацию через личный кабинет технической поддержки:

- уточните, появляется ли окно выбора сертификата пользователя, или ошибка появляется сразу;
- вышлите сертификаты пользователя и цепочку издателей в архивном файле;
- вышлите сертификаты пользователя и издателя. Для этого в КриптоПро CSP перейдите на вкладку «Сервис», нажмите кнопку «Просмотреть сертификаты в контейнере». Выберите закрытый ключ, нажмите кнопку «ОК», нажмите кнопку «Далее». В окне просмотра сертификата нажмите кнопку «Свойства». Перейдите на вкладку «Состав», нажмите кнопку «Копировать в файл». Сохраните сертификат на жесткий диск с помощью стандартного мастера выбора директории. После этого откройте файл сертификата. Перейдите на вкладку «Путь сертификации». Дважды нажмите на предпоследнее звено цепочки (где последнее нижнее звено – сертификат пользователя). Откроется сертификат Удостоверяющего центра издателя пользовательского сертификата. Перейдите на вкладку «Состав», нажмите кнопку «Копировать в файл» сохраните сертификат издателя. Вышлите в архивном файле сертификаты пользователя и издателя;
- логи ПО «Континент TLS VPN»;
- нажмите правой кнопкой мыши по пиктограмме ПО «Континент TLS VPN», нажмите кнопку «Журналы». Откроется оснастка «Просмотр событий». Раскройте раздел «Настраиваемые представления». В разделе отобразится пункт «События управления». Нажмите на него правой кнопкой мыши, выберите пункт «Сохранить все события в настраиваемом представлении как…» и следуйте указаниям мастера экспорта логов. Вышлите полученный evt(x)-файл в архивном файле.

Примечание – Экспорт настроек ПО «Континент TLS VPN». Выполняется в третьей вкладке данного ПО.

7.8 Получение инструкции, сертификата сервера и его издателя

Вопрос

Необходим порядок получения инструкции, сертификата сервера и его издателя для подключения ко ФГИС ЦС.

Ответ

Ознакомьтесь с официальной инструкцией: https://fgiscs.minstroyrf.ru/data-storage/enterInstruction.pdf.

Все необходимые сертификаты, согласно инструкции, доступны по ссылке: https://fgiscs.minstroyrf.ru/#/educationalMaterial.

7.9 Ошибка при подписании

Вопрос

При подписании документа возникают следующие ошибки:

– сообщение «Соединение прервано» (Рисунок 73);

– зависает кнопка «Подписать документ» (Рисунок 74).

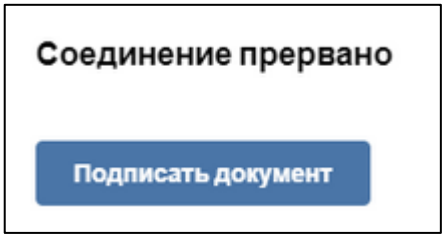

Рисунок 73 – Сообщение «Соединение прервано»

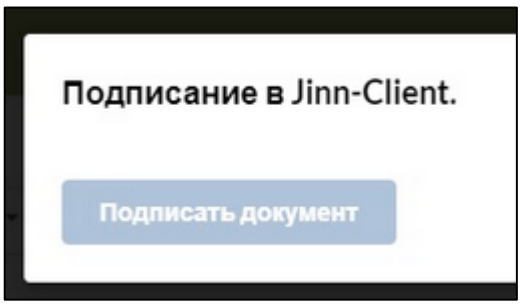

Рисунок 74 – Кнопка «Подписать документ»

Ответ

Для устранения данных ошибок выполните следующие действия:

– убедитесь, что ПО «Jinn-Client» инсталлирован в директорию «C:\Program Files\Security Code\Jinn-Client». Если это условие не выполняется, удалите ПО «Jinn-

Client» через пункт меню «Программы и компоненты» на Панели управления и повторно установите, указав директорию установки «C:\Program Files\Security Code\» и перейдите к следующему пункту. Если условие выполняется, сразу перейдите к следующему пункту;

- проверьте, отображается ли в окне «Программы и компоненты» (Пуск/Панель управления/Программы и компоненты) ПО «Jinn Sign Extension Provider». Если да, то переустановите ПО и проверьте, появится ли ошибка при установке. Если нет, сразу перейдите к установке;
- чтобы установить «Jinn Sign Extension Provider», запустите файл «JinnSignExtensionSetup.msi» и следуйте указаниям мастера установки. Если установка завершилась успешно, перейдите к следующему пункту. Если установка завершилась с ошибкой, удалите «Jinn Sign Extension Provider» через «Программы и компоненты» (Пуск/Панель управления/Программы и компоненты) (если такой там появился), и повторите установку, указав вручную директорию установки «C:\Program Files\Security Code\»;
- установите или переустановите плагин «Jinn Sign Extension» из магазина приложений Google Chrome.2.

Повторите попытку подписи. Если подпись не поставлена, пришлите скриншот ошибки и отчет по ПК, собранный утилитой «WinAudit». Скачать утилиту можно по ссылке: http://www.parmavex.co.uk/winaudit.html.

7.10 Ошибка при создании вектора энтропии

Вопрос

При создании вектора энтропии появляется сообщение об ошибке (Рисунок 75).

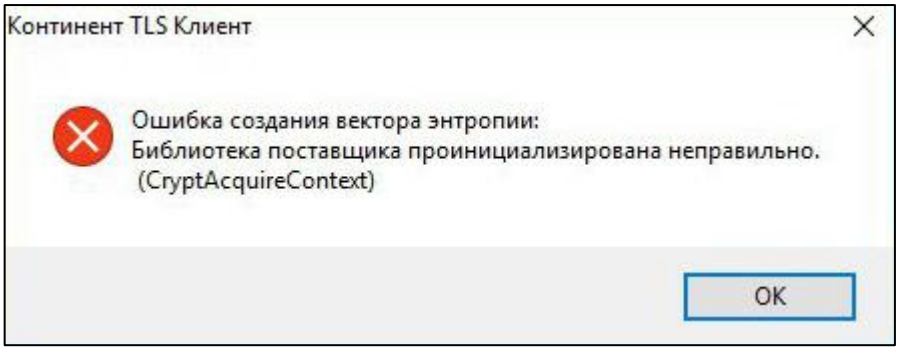

Рисунок 75 – Ошибка при создании вектора энтропии

Ответ

Данная ошибка может возникнуть в том случае, если на АРМ уже присутствуют другие криптопровайдеры («КриптоПро CSP2, «VipNet CSP2, «Signal-COM CSP» и т.д.). Во избежание данной ошибки устанавливайте СКЗИ «Jinn-Client», «Континент TLS VPN» на АРМ без прочих СКЗИ.

Примечание – Данная ошибка не является критической, и подключение во ФГИС ЦС возможно без создания вектора энтропии.

7.11 Установка ПО «Jinn-Client» без доверенной среды

Вопрос

При установке ПО «Jinn-Client» возникает сообщение, что ПО будет установлено в режиме lite.

Ответ

Сообщение о функционировании ПО «Jinn-Client» без доверенной среды является информационным (не критическим). Для работы во ФГИС ЦС наличие доверенной среды не требуется.

7.12 Пустая страница web-браузера

Вопрос

При переходе по https://fgiscs-tls.gge.ru:8443 сертификат запрашивается, после выбора сертификата вместо личного кабинета открывается пустая страница web-браузера.

Ответ

Данная ошибка возникает при подключении по протоколу http. Перезапустите web-браузер и перейдите по ссылке https://fgiscs-tls.gge.ru:8443 (обратите внимание, протокол https, его указание в адресной строке web-браузера обязательно).

7.13 Подключение не защищено

Вопрос

В web-браузере «Google Chrome» отображается сообщение «Ваше подключение не защищено» (Рисунок 76).

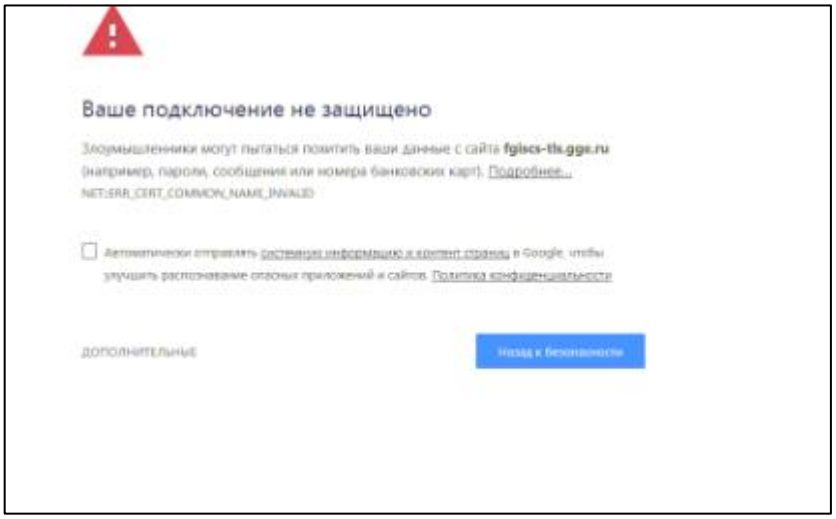

Рисунок 76 – Сообщение web-браузера «Google Chrome»

Ответ

Данная ошибка является ожидаемым поведением web-браузера «Google Chrome» и не является критической. При появлении данного сообщения нажмите на ссылку «Дополнительные», далее внизу страницы нажмите на ссылку «Перейти на сайт …». Отобразится страница портала.

Ознакомьтесь с файлом «Видеоинструкция по установке и настройке программного обеспечения Континент TLS VPN», где изображена данная процедура, доступным по ссылке https://fgiscs.minstroyrf.ru/#/educationalMaterial.

7.14 Несовместимость алгоритмов

Вопрос

После выбора сертификата пользователя появляется сообщение об ошибке: «Выбранный сертификат не соответствует сертификату сервера. Причина: несовместимость алгоритмов» (Рисунок 77).

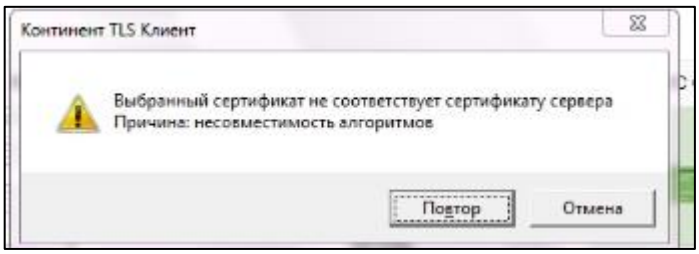

Рисунок 77 – Сообщение об ошибке

Ответ

Установите сборку ПО «Континент TLS VPN», доступную по ссылке: ftp://ftp.securitycode.ru\VENDOR-SUPPORT\5.TLS\1.2.1073.0.rar (загрузите дистрибутив либо с АРМ, где не установлено ПО «Континент TLS VPN», либо остановите службу «ContinentTLS», скачайте архив и снова запустите службу).

Для этого сначала удалите текущую версию через «Программы и компоненты», перезагрузите АРМ. Установите скачанную сборку, перезагрузите АРМ. Проверьте, что все выполненные ранее настройки сохранились. В противном случае, повторно настройте соединение по инструкции. Также в настройках соединения появится новое поле «Авторизация сервера по сертификату издателя». Установите «флажок» в данном поле.

Повторите попытку подключения к https://fgiscs-tls.gge.ru:8443.