Инструкция по настройке АРМ пользователя для работы с подсистемами ГИИС «Электронный бюджет» на базе 1С

СОДЕРЖАНИЕ

1 Список терминов и сокращений

Таблица 1. Термины и сокращения.

Термин/сокращение	Определение
АРМ	автоматизированное рабочее место пользователя
ОС	операционная система
ПО	программное обеспечение
Пользователь	зарегистрированный в системе сотрудник организации, которому предоставлен доступ к определенным функциям в БГУ и ЗКГУ, в соответствии с заявкой на подключение
СКЗИ	средство криптографической защиты информации
УЦ	удостоверяющий центр

2 Требования к АРМ пользователя и линиям связи

2.1 Технические требования к АРМ пользователей

АРМ пользователей должен соответствовать следующим требованиям к оборудованию:

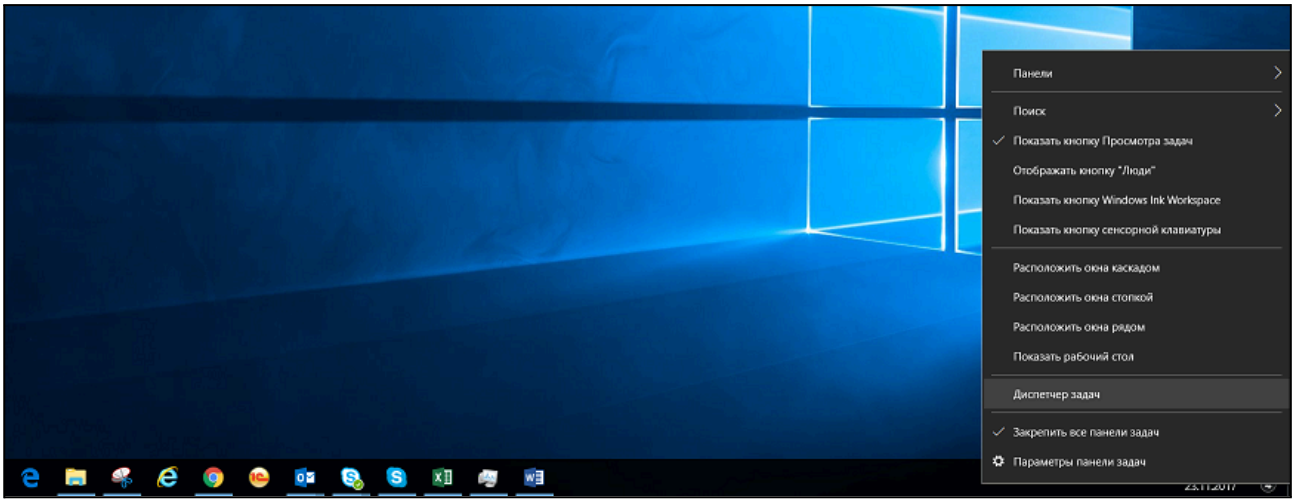
Процессор	Intel Core Duo 2400 МГц и выше
Оперативная память	от 4 Гб (от 1 Гб под 1С)
Жесткий диск	от 100Гб
Видеокарта	поддержка режима SVGA
Разрешение монитора	не менее 1600x1200

На АРМ пользователей должно быть установлено следующее программное обеспечение:

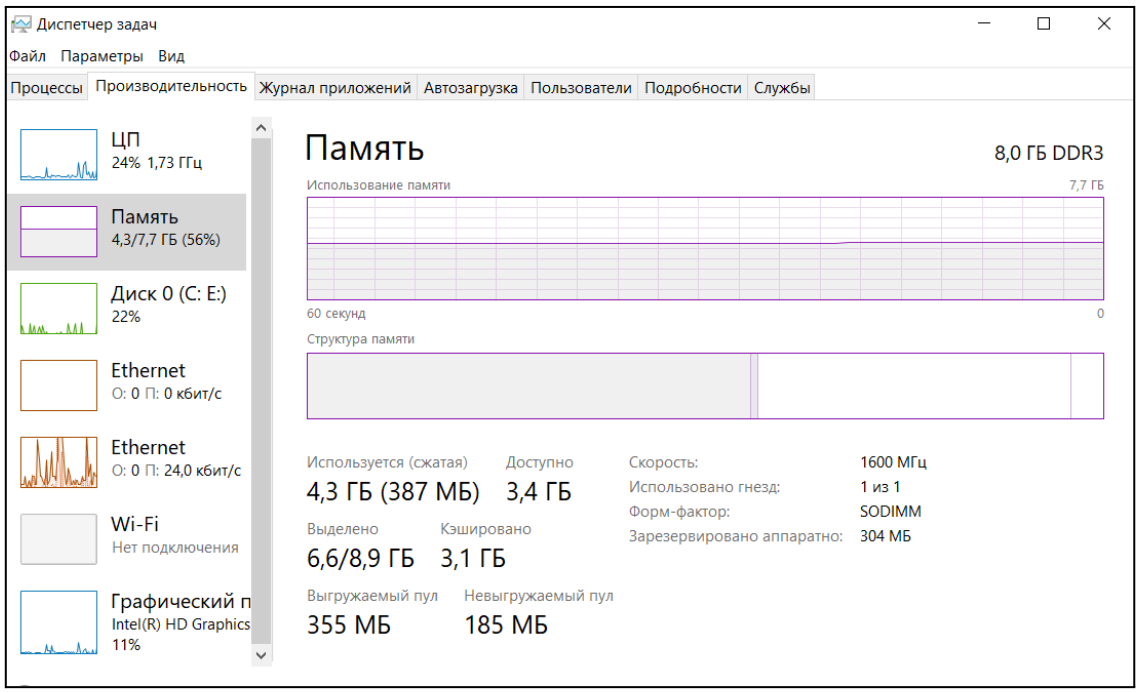
Операционная система	Windows 7 SP1 и выше
Браузер:	Microsoft Internet Explorer 11.0 Google Chrome (64-разрядные версии)

2.2 Проверка наличия достаточного количества свободной оперативной памяти

1. Правой кнопкой мыши вызвать контекстное меню панели задач и запустить Диспетчер задач:



2. Перейти на закладку «Производительность» и выбрать раздел «Память»



3. Размер «Доступной» памяти до запуска 1С должен быть не менее 1 ГБ.
4. В случае, если размер доступной памяти меньше 1ГБ, закройте работающие приложения: Документооборот, Word, Excel, веб-обозреватели и т.д.

2.3 Сертификаты

Для работы у пользователя должны быть в наличии следующие сертификаты:

1) Корневой сертификат Минкомсвязь России, выданного Минкомсвязь России.
2) Промежуточный сертификат Федерального казначейства, выданного Минкомсвязь России. Сертификат можно скачать с официального сайта Федерального казначейства в разделе ГИС/Удостоверяющий центр/Корневые сертификаты (https://roskazna.ru/gis/udostoveryayushhij-centr/kornevye-sertifikaty/)
3) Сертификат сайта buh2012.budget.gov.ru (для доступа посредством Континент ТЛС клиент). Сертификат сайта можно скачать с официального сайта Федерального казначейства в разделе ГИС/Электронный бюджет/Подключение к системе (https://roskazna.ru/gis/ehlektronnyj-byudzhet/podklyuchenie-k-sisteme/)

4) Квалифицированный сертификат пользователя 2012 ГОСТ.

3 Технические требования к каналам

Между АРМ пользователей и ЦОД необходимо обеспечить канал связи со скоростью не менее 3 Мбит/с.

4 Настройка рабочего места

4.1 Удаление криптопровайдера

В случае наличия на АРМ устаревших версий криптопровайдера, необходимо их удалить.

4.1.1 КриптоПро CSP

После удаления КриптоПРО CSP рекомендуется запустить специализированное приложение КриптоПРО для очистки cspclean.exe.

4.1.2 Код безопасности CSP

После удаления Кода безопасности CSP рекомендуется запустить специализированное приложение Кода Безопасности для очистки cspcleaner.exe.

4.2 Установка корневого сертификата в локальное хранилище компьютера

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

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

На экране отобразится мастер импорта сертификатов.

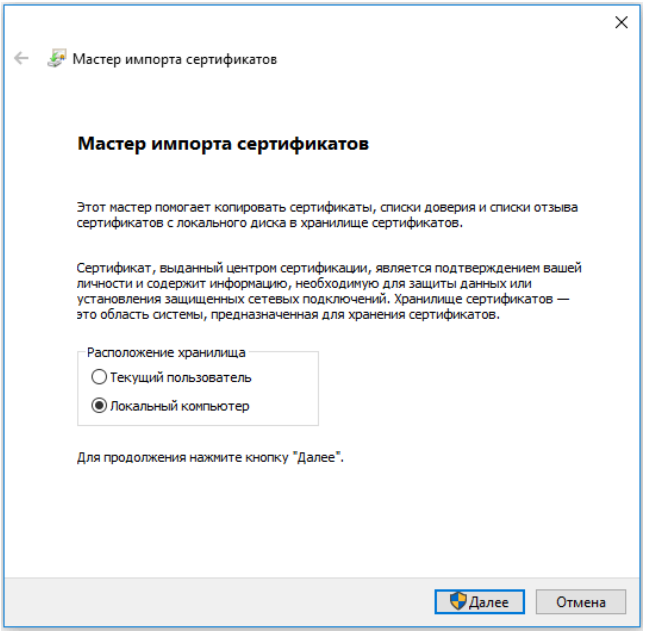


Рисунок 4.1. Мастер импорта сертификатов

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

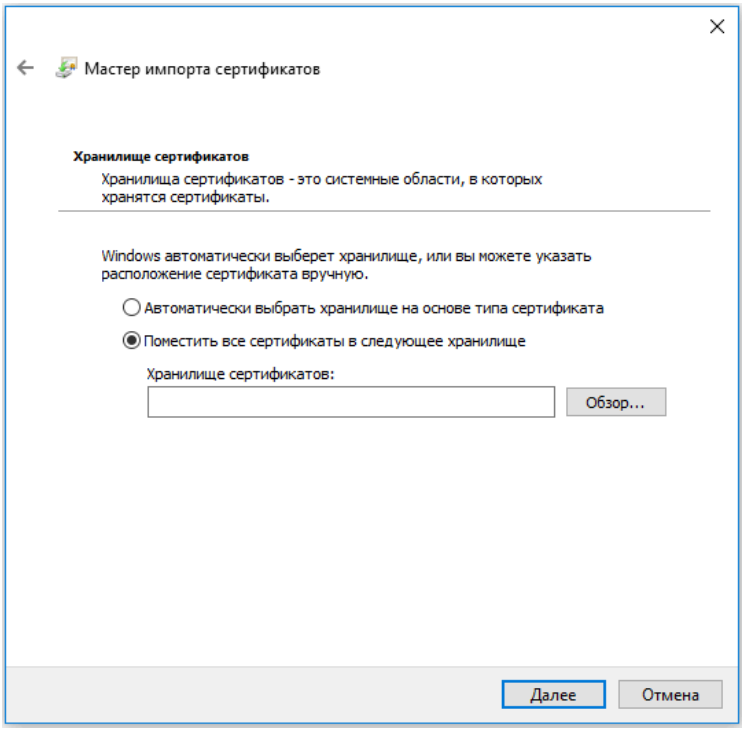


Рисунок 4.2. Выбор хранилища сертификата

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

4) Нажать кнопку «Обзор…». Откроется окно «Выбор хранилища сертификата».

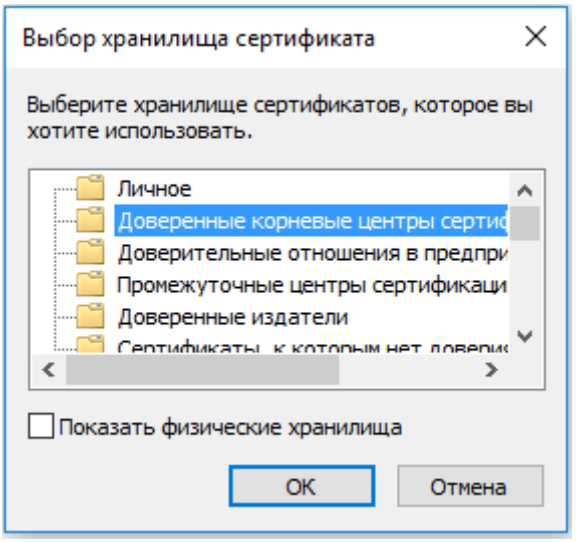


Рисунок 4.3. Выбор хранилища сертификата

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

Откроется окно завершения работы мастера импорта сертификатов.

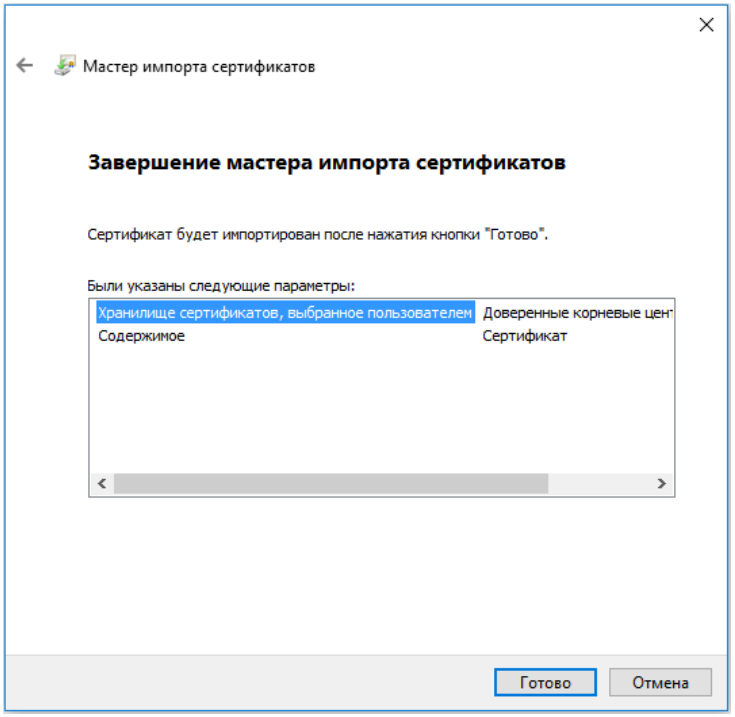


Рисунок 4.4. Окно завершения работы мастера импорта сертификатов

6) Нажать кнопку «Готово».

Появится сообщение, что импорт успешно выполнен.

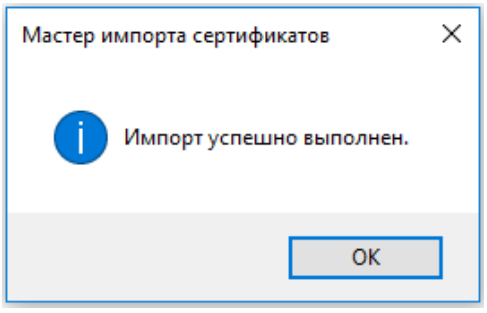


Рисунок 4.5. Завершение установки

7) Нажать кнопку «ОК».

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

4.3 Установка промежуточного сертификата в локальное хранилище компьютера

Для установки промежуточного сертификата в хранилище сертификатов компьютера средствами операционной системы семейства Windows

необходимо:

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

На экране отобразится мастер импорта сертификатов.

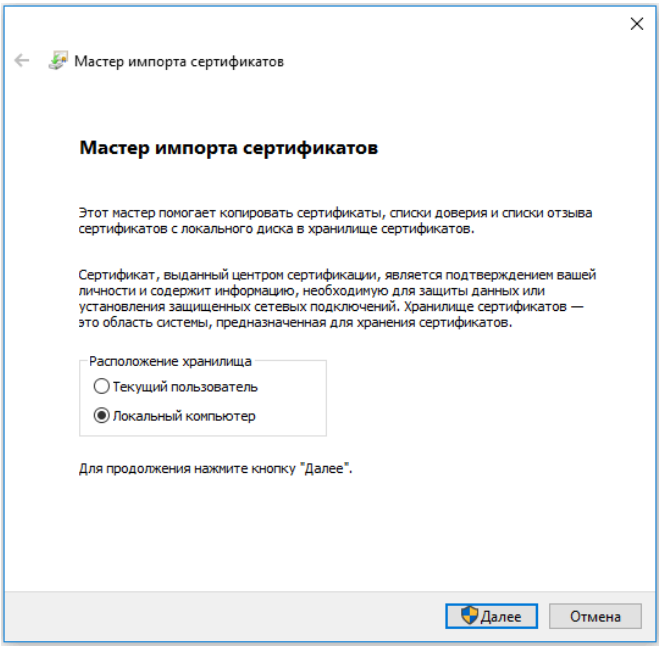


Рисунок 4.6. Мастер импорта сертификатов

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

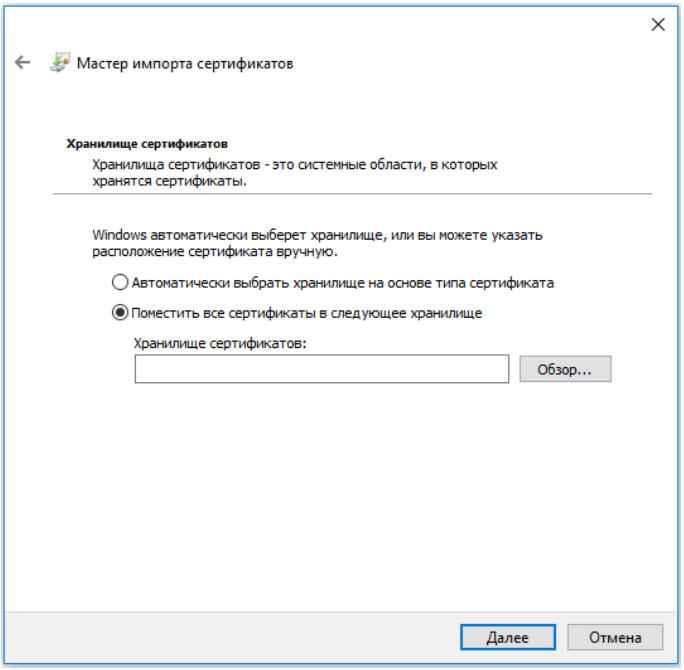


Рисунок 4.7. Выбор хранилища сертификата

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

10) Нажать кнопку «Обзор…». Откроется окно «Выбор хранилища сертификата».

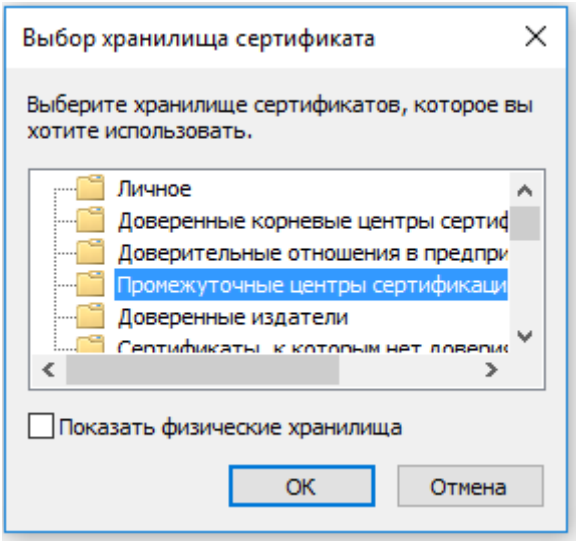


Рисунок 4.8. Выбор хранилища сертификата

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

Откроется окно завершения работы мастера импорта сертификатов.

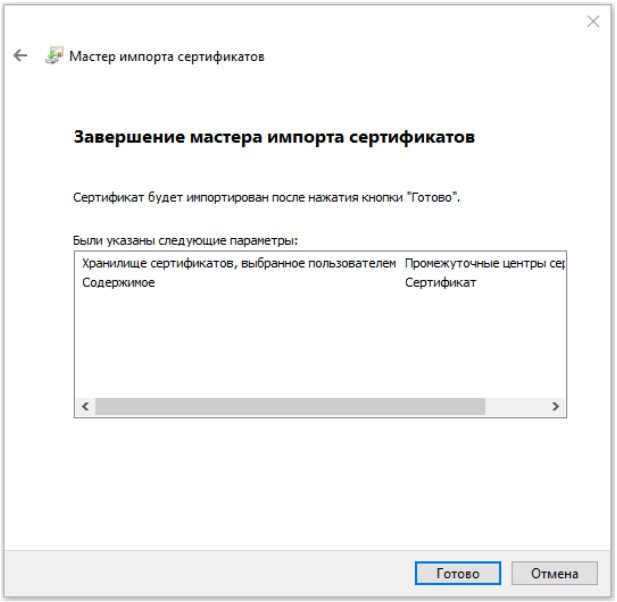


Рисунок 4.9. Окно завершения работы мастера импорта сертификатов

12) Нажать кнопку «Готово».

Появится сообщение, что импорт успешно выполнен.

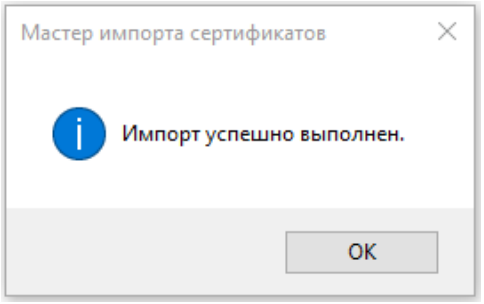


Рисунок 4.10. Завершение установки

13) Нажать кнопку «ОК».

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

4.4 Установка и настройка криптопровайдера КриптоПро CSP

4.4.1 Установка КриптоПро CSP 4.0 необходима в случаях:

a) для работы с использованием ключа ЭП 2012 ГОСТ, созданного в КриптоПРО

b) для работы в браузере Internet Explorer без установки Континент TLS клиента.

4.4.2 В случае отсутствия дистрибутива необходимо обратиться в ОРСиБИ Федерального казначейства своего региона.

4.4.3 Для установки криптопровайдера КриптоПро CSP необходимо:

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

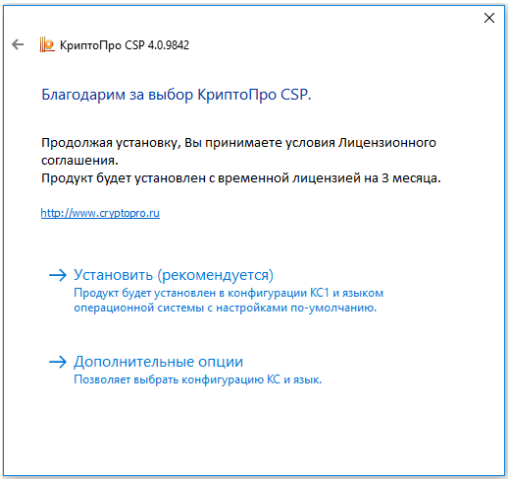


Рисунок 4.11 Стартовое окно мастера установки КриптоПро CSP

14) Нажать кнопку «Установить (рекомендуется)». Отобразится окно процесса установки КриптоПро CSP.

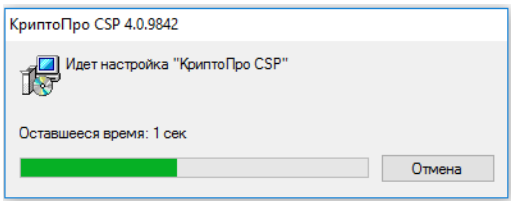


Рисунок 4.12. Процесс установки КриптоПро CSP

15) После успешной установки криптопровайдера отобразится диалог «КриптоПро CSP успешно установлен».

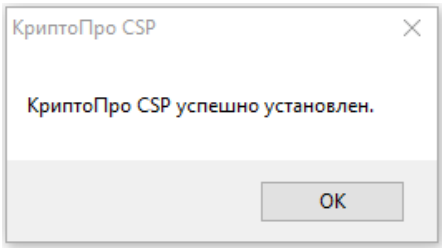


Рисунок 4.13. Успешная установка КриптоПро CSP

16) Нажать кнопку «ОК».

17) Запустить КриптоПро CSP. Во вкладке общие нажать кнопку «Ввод лицензии» и ввести лицензионный ключ.

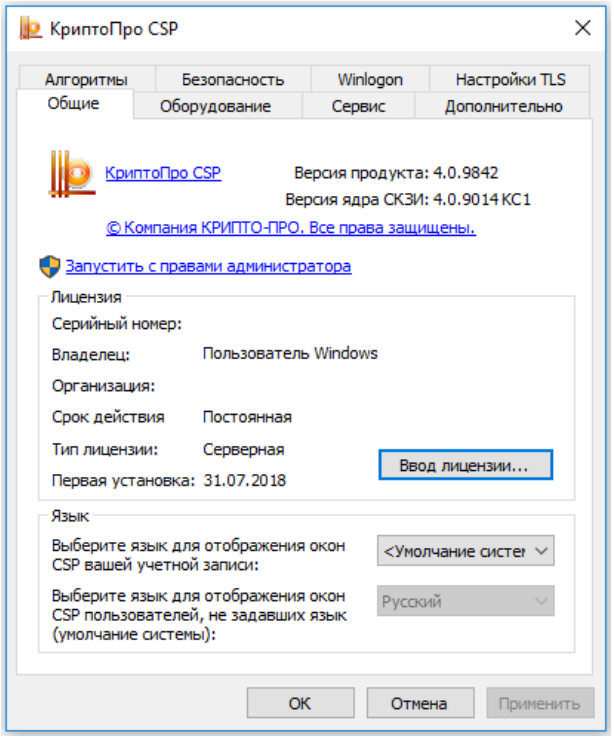


Рисунок 4.14. Вкладка «Общие». КриптоПро CSP

4.4.4 Для настройки криптопровайдера необходимо выполнить следующие действия:

1) Запустить КриптоПро CSP от имени Администратора.

18) Перейти во вкладку «Настройки TLS».

19) Отметить в разделе «Клиент» следующие чекбоксы:

- Не проверять сертификат сертификат сервера на отзыв
- Не проверять назначение собственного сертификата

И снимите галочку в блоке «Клиент» для поля «Не использовать устаревшие cipher suite-ы»:

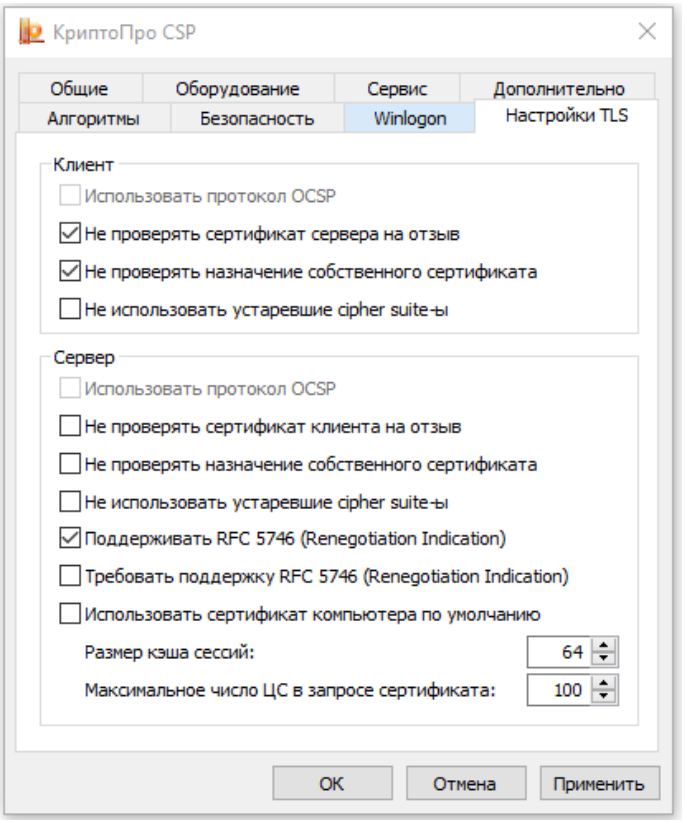


Рисунок 4.15. Вкладка «Настройки TLS». КриптоПро CSP

20) Нажать кнопку «Применить».

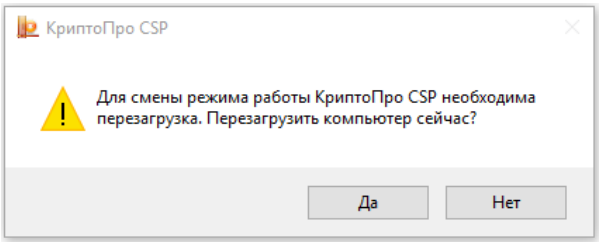


Рисунок 4.16. Запрос на перезагрузку после смены режима работы

Появится запрос на перезагрузку АРМ.

21) Нажать кнопку «Да». АРМ перезагрузится.

4.5 Установка сертификата пользователя, созданного в КриптоПро, в хранилище личных сертификатов АРМ пользователя (при необходимости)

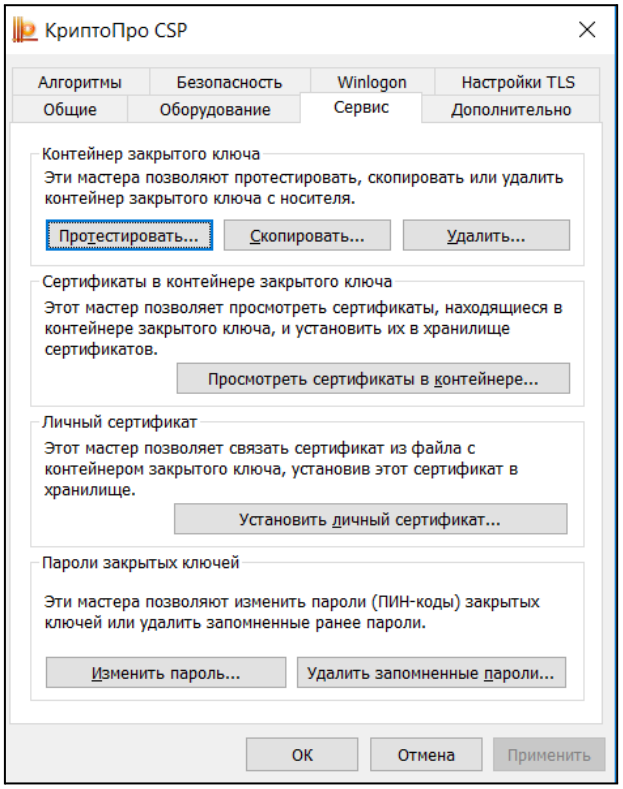
4.5.1 Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется в случае, если файл сертификата пользователя не является единым целым с закрытым ключом (в процессе получения в УЦ

сертификат в формате «*.cer» был записан на отдельный носитель информации).

4.5.2 Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в личный кабинет БГУ 2.0 и ЗКГУ 3.0.

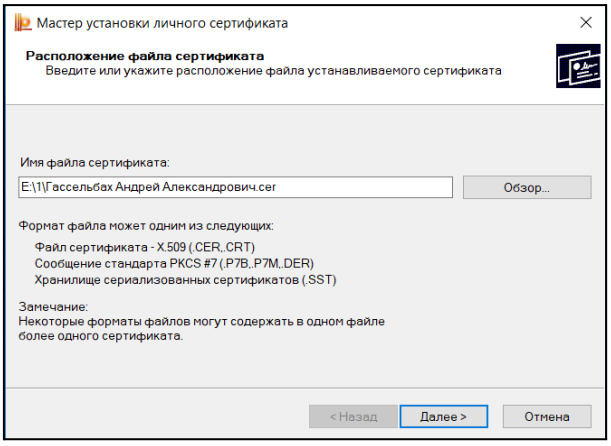
4.5.3 Для установки квалифицированного сертификата пользователя необходим запустить КриптоПро CSP:

1) Перейти на вкладку «Сервис»:

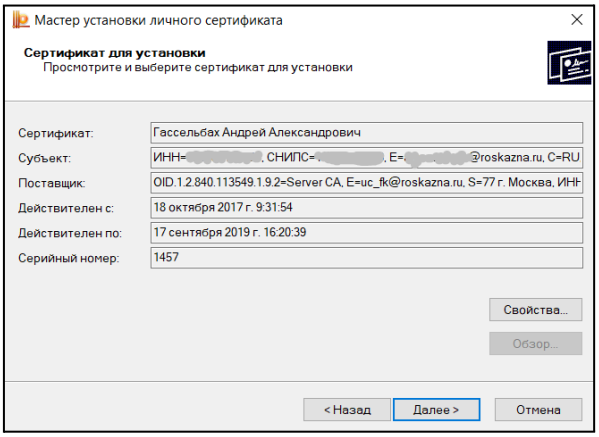


22) Нажать кнопку «Установить личный сертификат …»

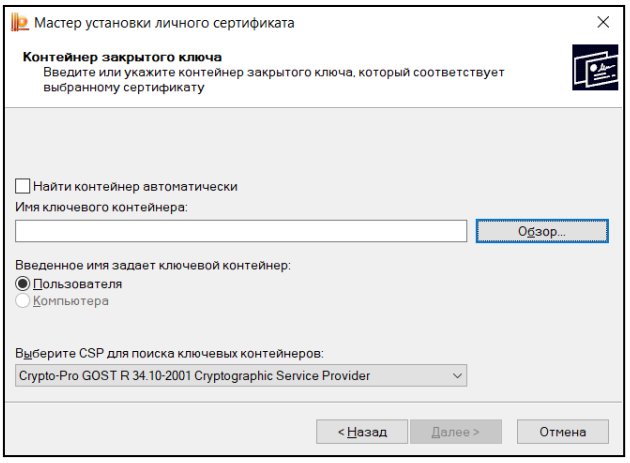
23) В открывшемся окне мастера установки личного сертификата указать место размещения сертификата на АРМ пользователя, и нажать кнопку «Далее»:



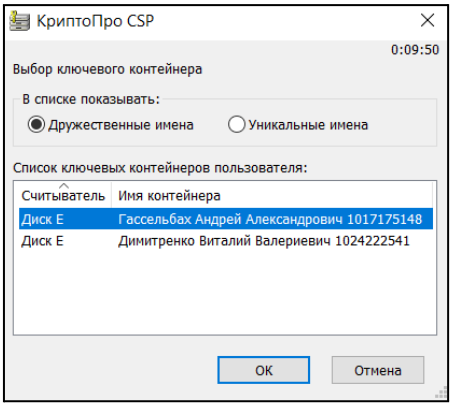
24) Открывается окно просмотра сертификата для установки. Нажмите кнопку «Далее»:



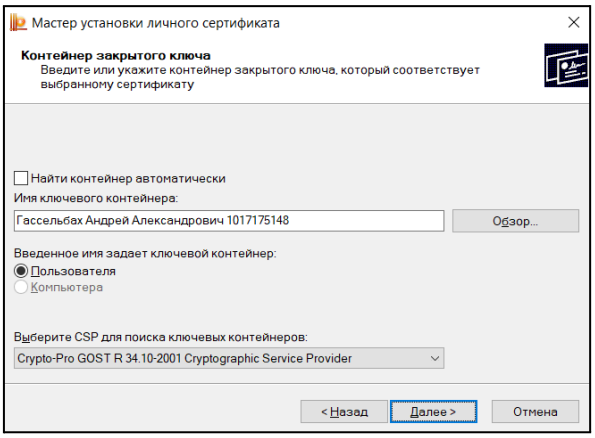
25) В открытом окне выбора Контейнера закрытого ключа нажмите кнопку «Обзор»:



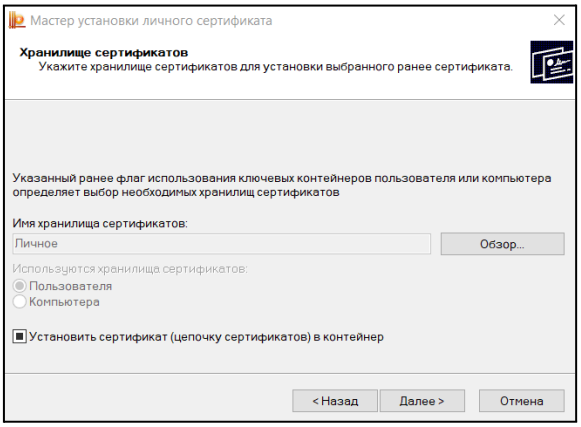
26) В открывшемся окне укажите контейнер и нажмите кнопку «Ок»:



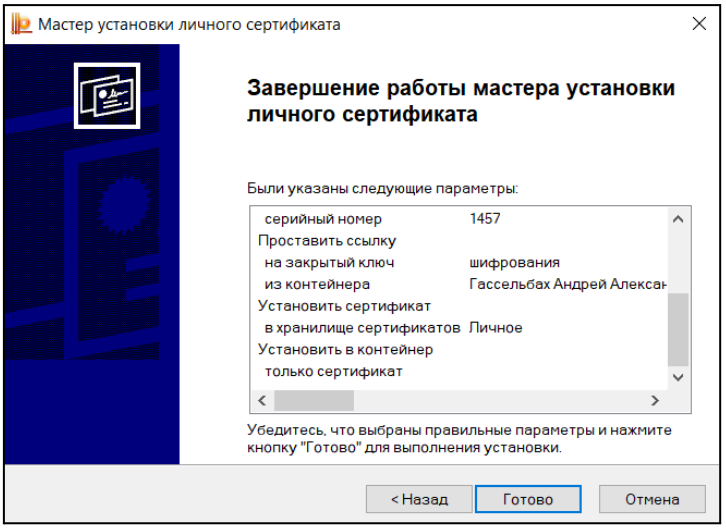
27) В окне выбора контейнера закрытого ключа нажмите кнопку «Далее»:



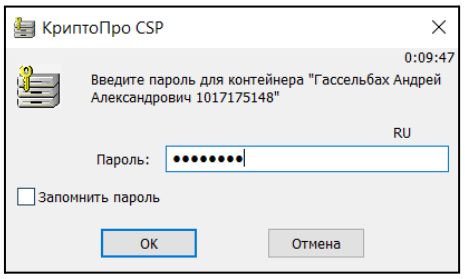
28) В открытом окне указания хранилища сертификатов нажмите кнопку «Далее»:



29) В окне завершения работы мастера установки личного сертификата нажмите кнопку «Готово»



30) Введите пароль для контейнера закрытого ключа и нажмите кнопку «Ок»:



31) Импорт завершен

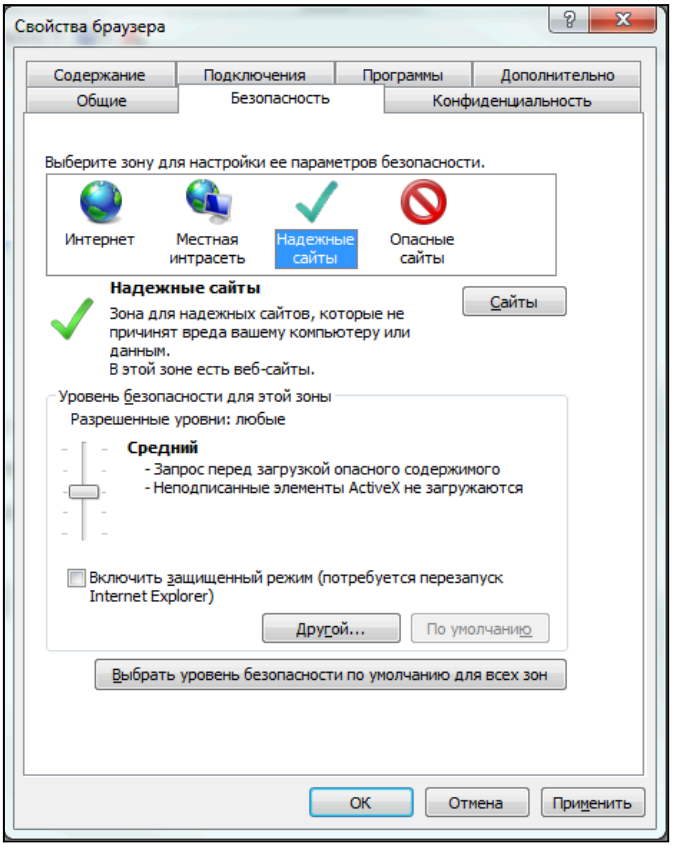
4.6 Настройка веб-обозревателя Internet Explorer для работы без установки Континент TLS клиент.

4.6.1 Установите сертификат сайта в локальное хранилище компьютера как «Доверенные лица» по аналогии с п.4.3.

4.6.2 Настройка веб-обозревателя Internet Explorer для подключения к БГУ 2 и ЗКГУ 3 состоит из следующих шагов.

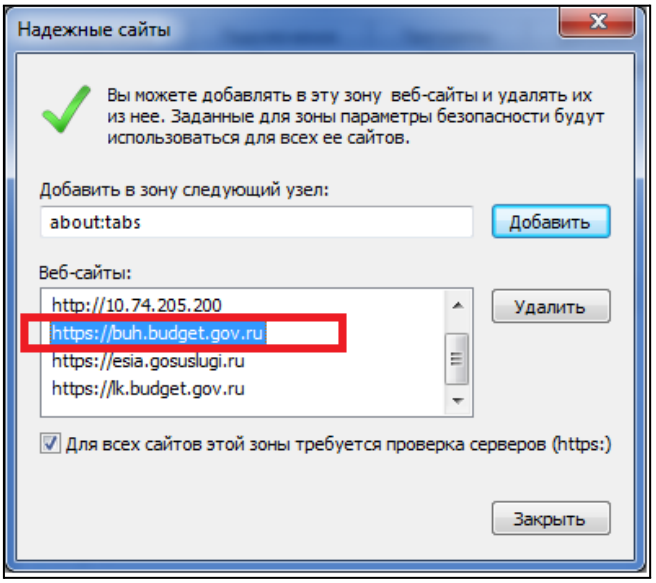
1) Открыть свойства веб-обозревателя.

32) Перейти на вкладку «Безопасность».



33) Выбрать зону для настройки «Надежные узлы».

34) Нажать кнопку «Сайты».



35) В окне «Надежные сайты» снять отметку с поля «Для всех сайтов этой зоны требуется проверка серверов (https:)».

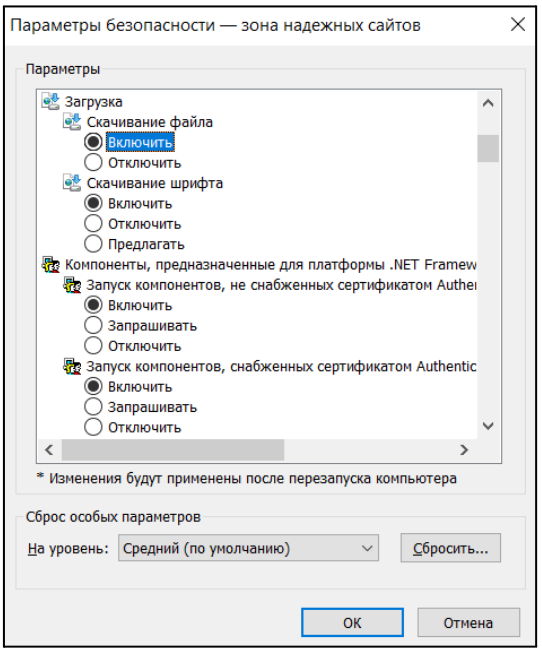
36) В поле «Добавить в зону следующий узел» задать значение «https://*.budget.gov.ru» и нажать кнопку «Добавить»

37) В окне «Надежные сайты» нажать кнопку «Закрыть».

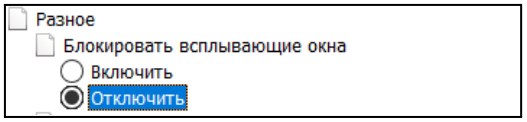
38) На вкладке «Безопасность» в зоне для настройки «Надежные узлы» нажать кнопку «Другой»

39) В окне «Параметры безопасности – зона надежных сайтов» установить:

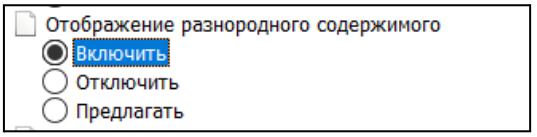
a) в разделе «Загрузка» параметр «Скачивание файла» в положение «Включить»



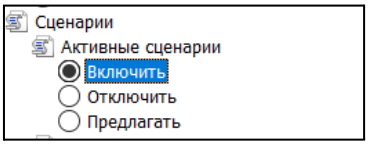
c) в разделе «Разное» параметр «Блокирование всплывающих окон» в положение «Отключить»



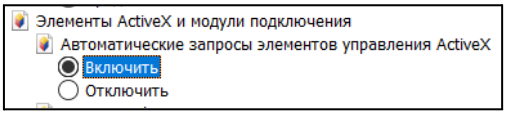
d) в разделе «Разное» параметр «Отображение разнородного содержимого» в положение «Включить»



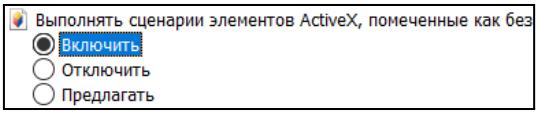
e) в разделе «Сценарии» параметр «Активные сценарии» в положение «Включить»



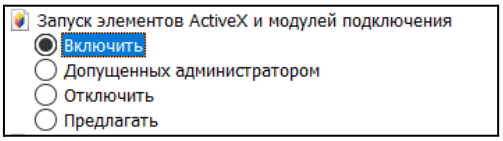
f) в разделе «Элементы ActiveX и модули подключения» параметр «Автоматические запросы элементов управления ActiveX» в положение «Включить»



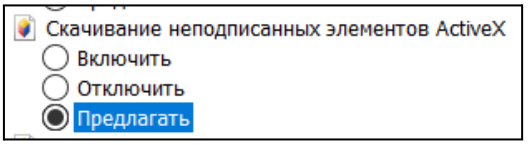
g) в разделе «Элементы ActiveX и модули подключения» параметр «Выполнять сценарии элементов ActiveX, помеченные как безопасные*» в положение «Включить»



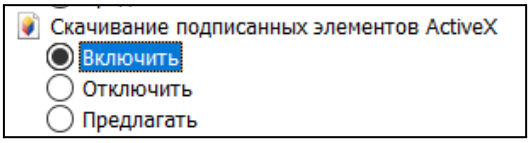
h) в разделе «Элементы ActiveX и модули подключения» параметр «Запуск элементов ActiveX и модулей подключения» в положение «Включить»



i) в разделе «Элементы ActiveX и модули подключения» параметр «Скачивание неподписанных элементов ActiveX» в положение «Предлагать»

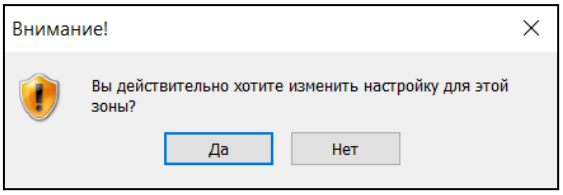


j) в разделе «Элементы ActiveX и модули подключения» параметр «Скачивание подписанных элементов ActiveX» в положение «Включить»

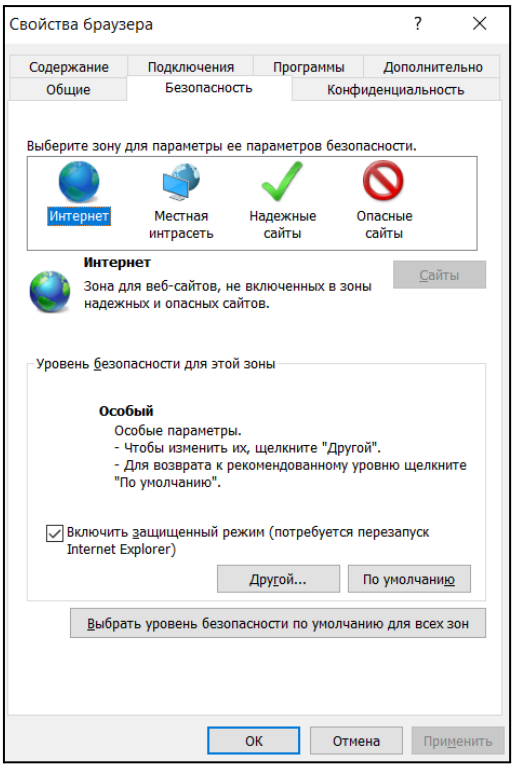


40) В окне «Параметры безопасности – зона надежных сайтов» нажать кнопку «Ок».

41) В открывшемся окне «Внимание!» нажать кнопу «Да».

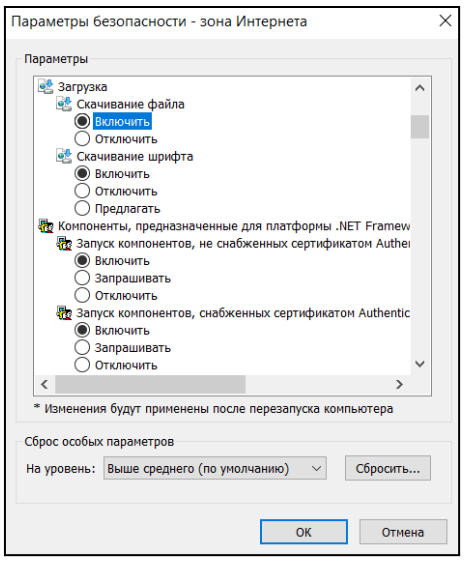


42) Выбрать зону для настройки «Интернет» и нажать кнопку «Другой»

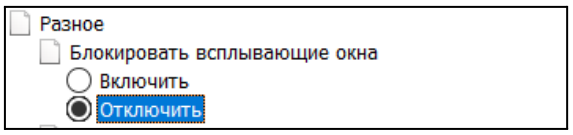


43) В окне «Параметры безопасности – зона Интернет» установить:

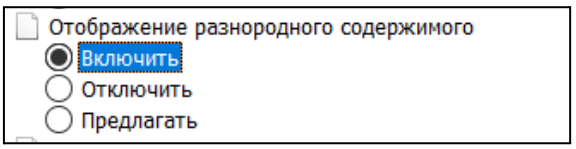
a) в разделе «Загрузка» параметр «Скачивание файла» в положение «Включить»



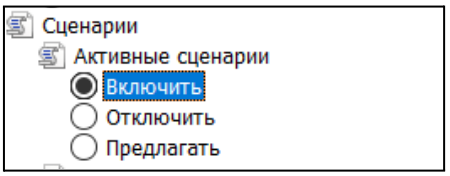
k) в разделе «Разное» параметр «Блокирование всплывающих окон» в положение «Отключить»



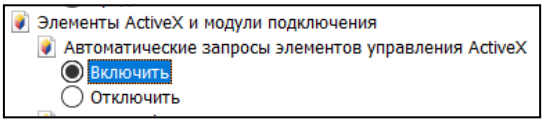
l) в разделе «Разное» параметр «Отображение разнородного содержимого» в положение «Включить»



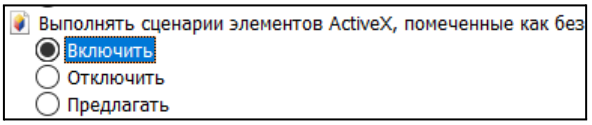
m) в разделе «Сценарии» параметр «Активные сценарии» в положение «Включить»



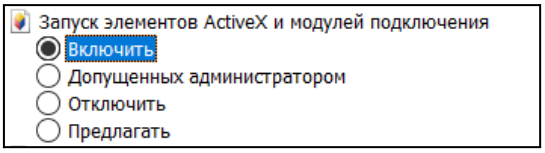
n) в разделе «Элементы ActiveX и модули подключения» параметр «Автоматические запросы элементы управления ActiveX» в положение «Включить»



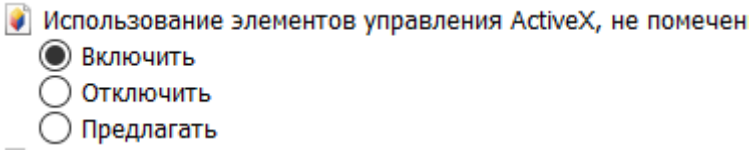
o) в разделе «Элементы ActiveX и модули подключения» параметр «Выполнять сценарии элементов ActiveX, помеченные как безопасные*» в положение «Включить»



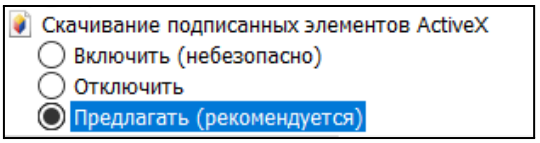
p) в разделе «Элементы ActiveX и модули подключения» параметр «Запуск элементов ActiveX и модулей подключения» в положение «Включить»



q) в разделе «Элементы ActiveX и модули подключения» параметр «Использование элементов управления ActiveX, не помеченных как безопасные для использования» в положение «Включить»

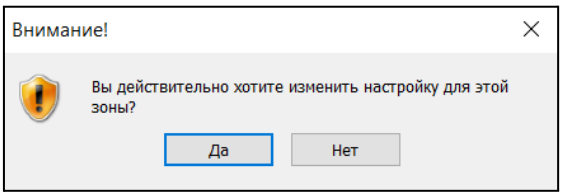


r) в разделе «Элементы ActiveX и модули подключения» параметр «Скачивание подписанных элементов ActiveX» в положение «Предлагать (рекомендуется)»

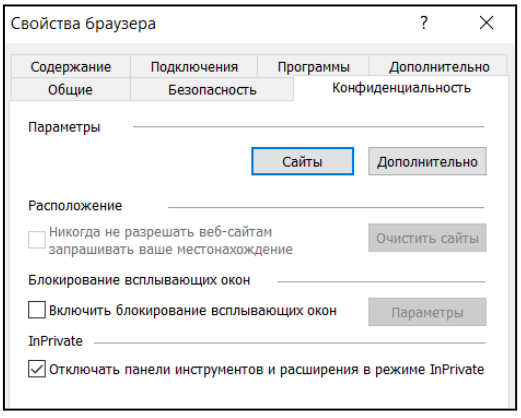


44) В окне «Параметры безопасности – зона Интернета» нажать кнопку «Ок».

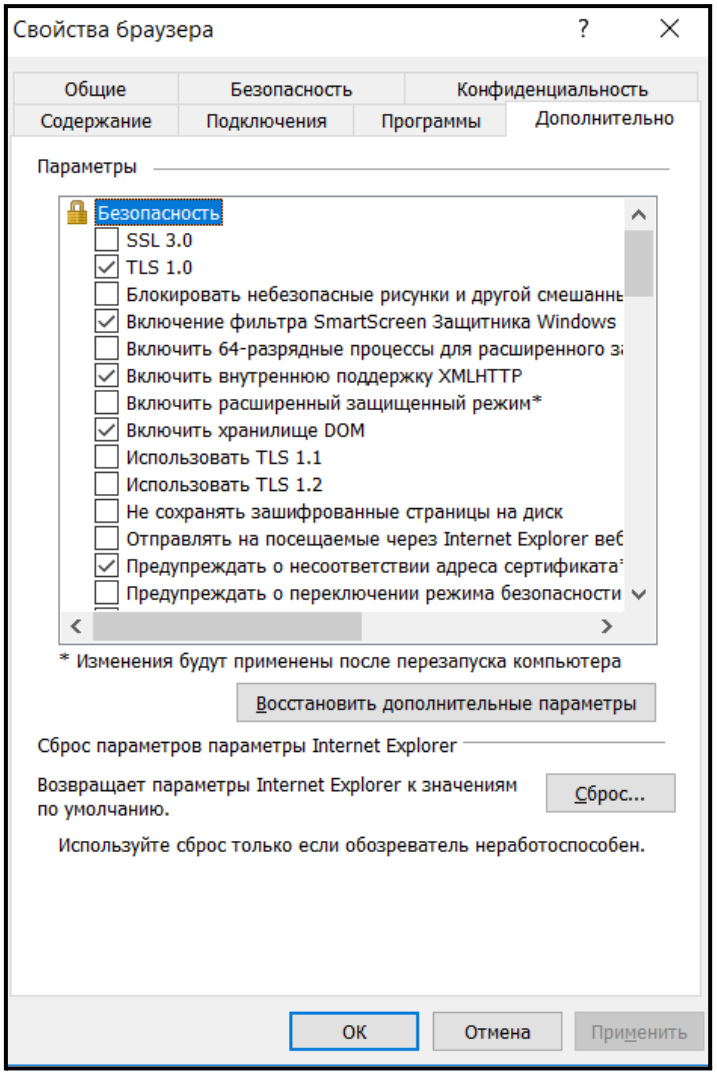
45) В открывшемся окне «Внимание!» нажать кнопу «Да».



46) Перейти на вкладку «Конфиденциальность» и отключить параметр «Включить блокирование всплывающих окон» в соответствии с рисунком:



47) Перейти на вкладку «Дополнительно» и настроить параметры безопасности «TLS 1.0», «Использовать TLS 1.1», «Использовать TLS 1.2», «Включить хранилище DOM» в соответствии с рисунком:



48) В окне «Свойства браузера» нажать кнопку «ОК».

49) Закрыть веб-обозреватель.

50) Перезагрузить АРМ

4.7 Установка СКЗИ «Континент TLS VPN Клиент»

4.7.1 Подготовка к установке

Необходимость установки СКЗИ «Континент TLS VPN Клиент» для работы в Личном кабинете Электронного бюджета обусловлена возможностью эксплуатации браузеров, отличных от Internet Explorer.

В случае отсутствия дистрибутива необходимо обратиться в ОРСиБИ Федерального казначейства своего региона.

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

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

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

Если на АРМ пользователя ранее был установлен криптопровайдер Код Безопасности CSP, который мог устанавливаться отдельно или был встроен в предыдущие версии каких-либо продуктов от производителя «Код Безопасности», то перед началом установки новой версии Континент TLS Клиента требуется удалить остаточные файлы криптопровайдера.

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

4.7.2 Установка СКЗИ «Континент TLS VPN Клиент»

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

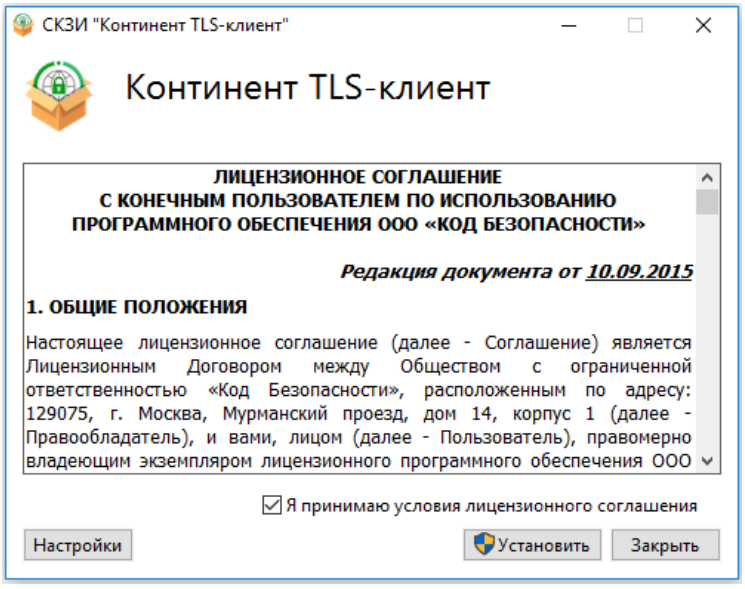


Рисунок 4.17. Стартовое окно мастера установки СКЗИ «Континент TLS VPN Клиент»

51) Отметить чекбокс «Я принимаю условия лицензионного соглашения». Нажать кнопку «Установить».

Начнется процесс установки.

52) При успешной установке отобразится диалоговое окно «Установка завершена».

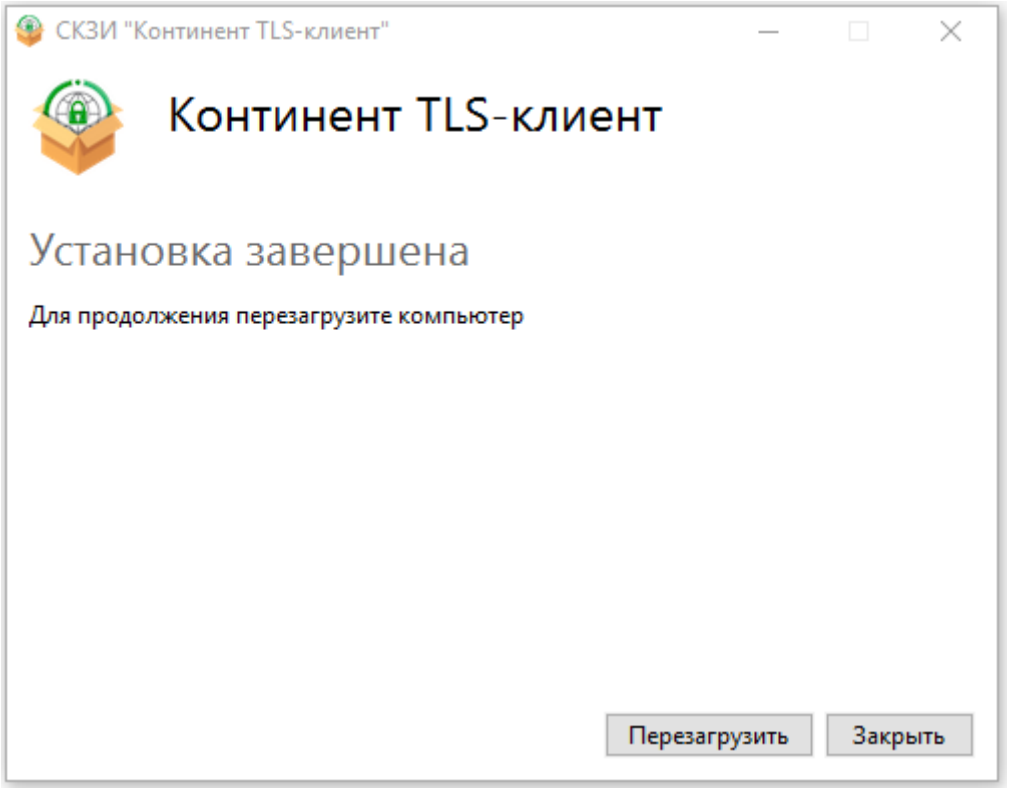


Рисунок 4.18. Диалоговое окно завершения установки

53) Нажмите кнопку «Перезагрузить». АРМ перезагрузится.

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

4.7.3 Регистрация СКЗИ «Континент TLS VPN Клиент»

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

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

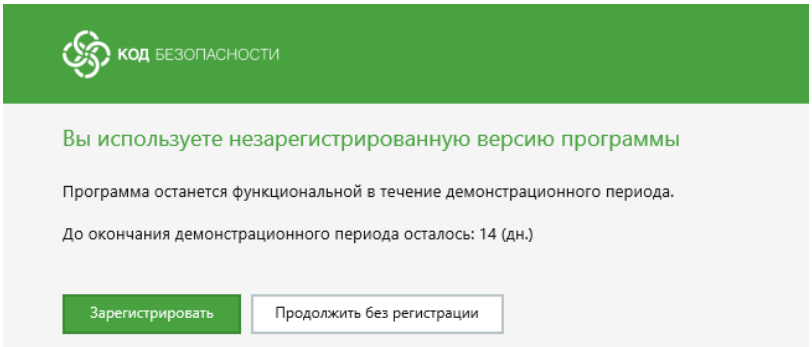


Рисунок 4.19. Диалоговое окно о состоянии регистрации СКЗИ

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

4.7.3.1 Регистрация через интернет

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

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

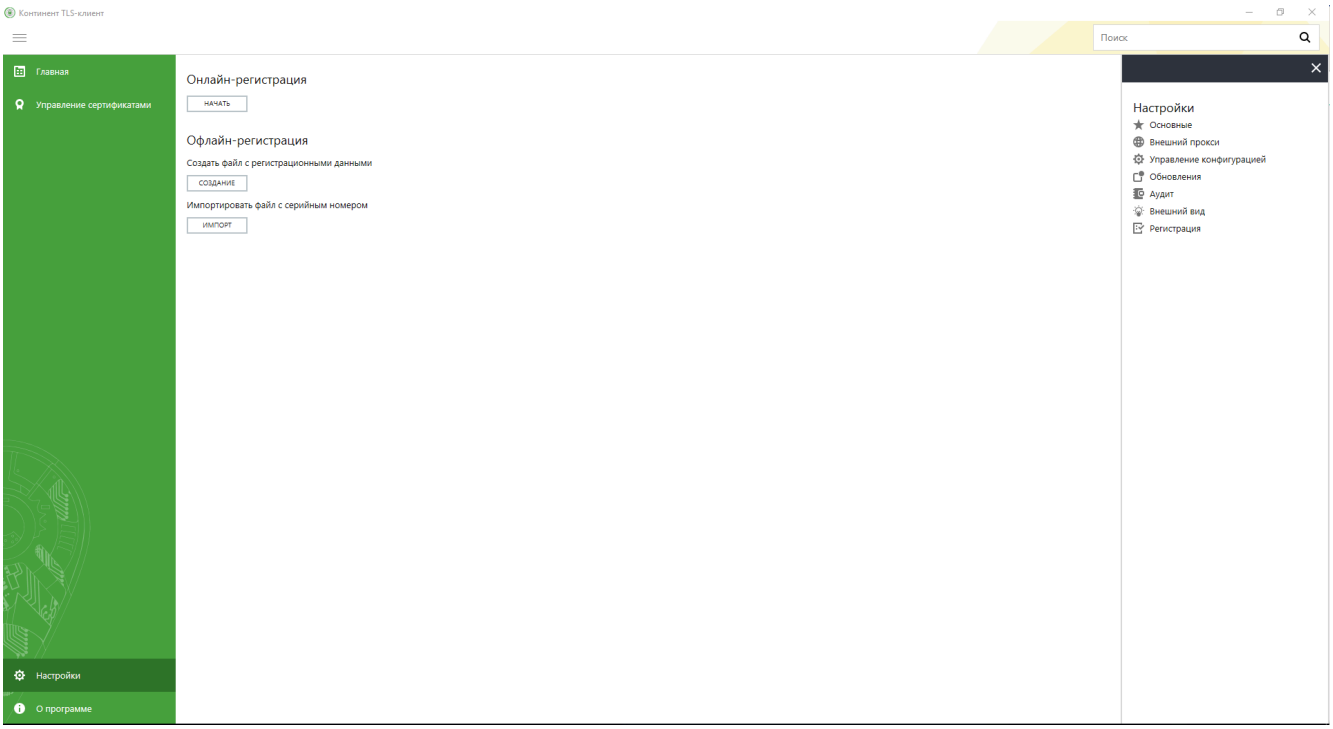


Рисунок 4.20. Вкладка «Настройки», раздел «Регистрация». Континент TLS Клиент

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

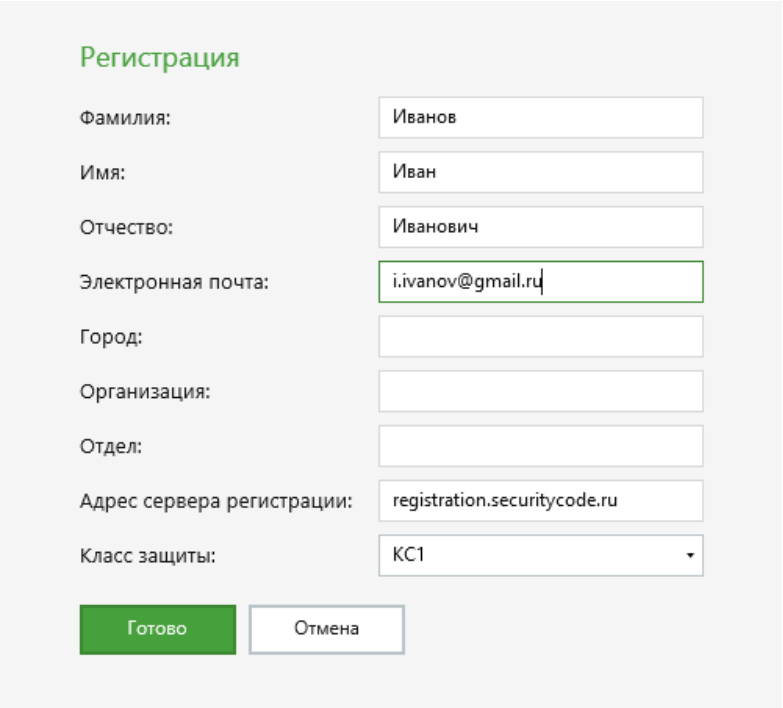


Рисунок 4.21. Окно регистрации СКЗИ

55) Нажать кнопку «Готово».

4.7.3.2 Регистрация без интернет

В случае если доступ к системе производится из сети ЗКВС Федерального казначейства, необходимо осуществить офлайн-регистрацию.

Для этого на рабочем месте пользователя необходимо выполнить следующие действия:

1) Нажать комбинацию клавиш «WIN + R».

56) В зависимости от используемой на АРМ операционной системы в появившемся окне ввести строку:

   a) Для ОС Windows XP: %ALLUSERSPROFILE%\\ContinentTLSClient\\ и нажать кнопку «ОК»,

   b) Для ОС Windows 7 и выше: %PUBLIC%\\ContinentTLSClient\\ и нажать кнопку «ОК».

57) В открывшейся папке открыть на редактирование (с помощью Блокнота или Notepad++) файл PublicConfig.json.

Файл откроется со следующим содержимым:

```
{
 "loggingConfig": {
    "fileLogMaxSize": 3145728,
    "fileLoggingDirectory": "C:\\Users\\Public\\ContinentTLSClient\\",
    "fileLoggingEnabled": true,
    "sessionLogsEnabled": false
 },
 "serialNumber": ""
}
```


58) Для регистрации необходимо заполнить поле serialNumber значением «test-50000».

4.8 Установка jinn-client

4.8.1 Установка Jinn-Clinet

4.8.1.1 В случае отсутствия дистрибутива необходимо обратиться в ОРСиБИ Федерального казначейства своего региона.

4.8.1.2 Рекомендуемая сборка СКЗИ «Jinn-Client» 1.0.3050.0.

4.8.1.3 Для установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» необходимо:

1) В АРМ пользователя вставить носитель информации, содержащий дистрибутив СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

59) В составе дистрибутива СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» осуществить запуск исполняемого файла «Setup.exe». На экране отобразится меню единого установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

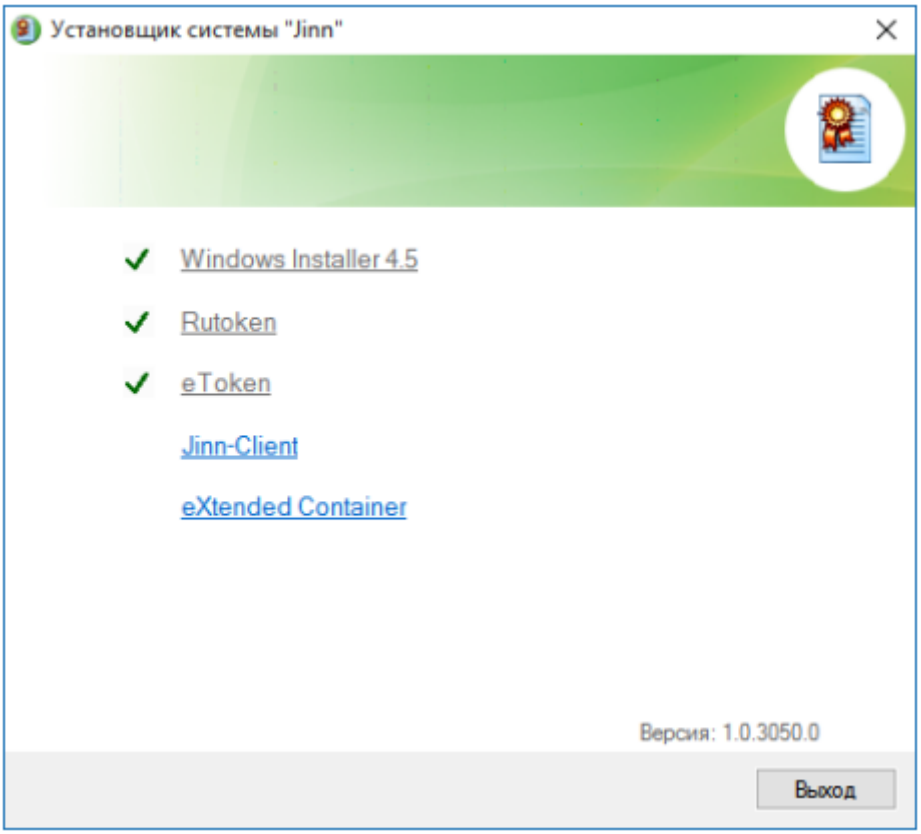


Рисунок 4.22. Меню единого установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

60) В меню установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» активировать ссылку «Jinn-Client». На экране отобразится диалог приветствия установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

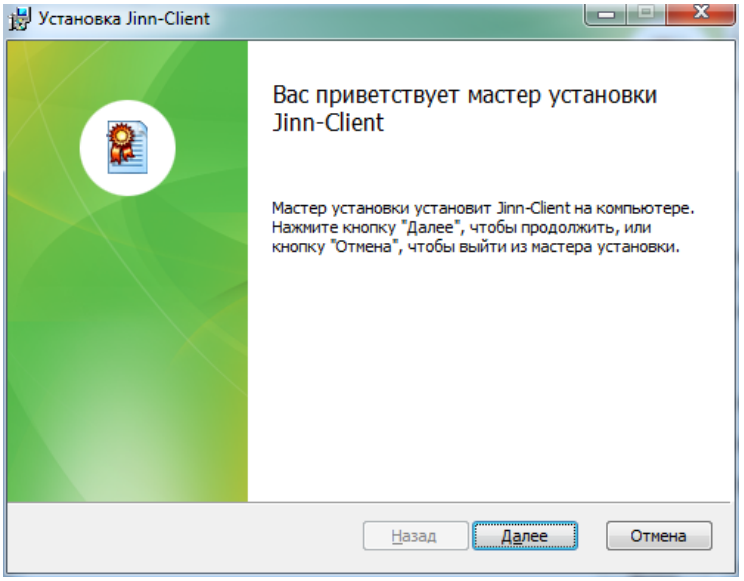


Рисунок 4.23. Окно приветствия установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

61) Для продолжения установки нажмите кнопку «Далее».

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

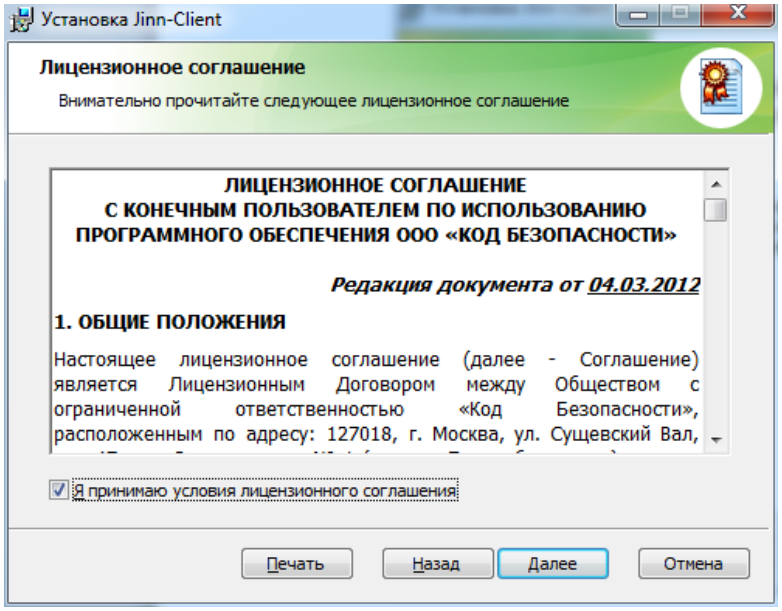


Рисунок 4.24. Окно просмотра лицензионного соглашения

63) На экране отобразится диалог ввода лицензионного ключа, поставляемого вместе с дистрибутивом СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» в электронном или бумажном виде.

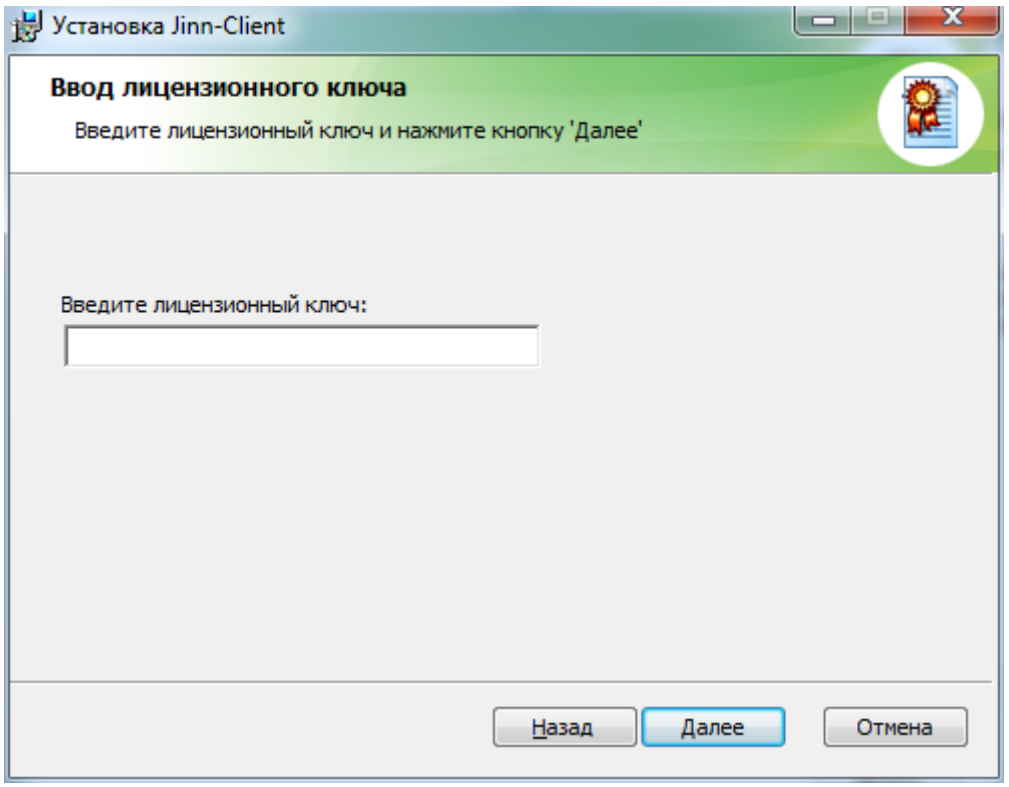


Рисунок 4.25. Окно ввода лицензионного ключа

64) Введите лицензионный ключ и нажмите кнопку «Далее». На экране отобразится диалог выбора пути установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

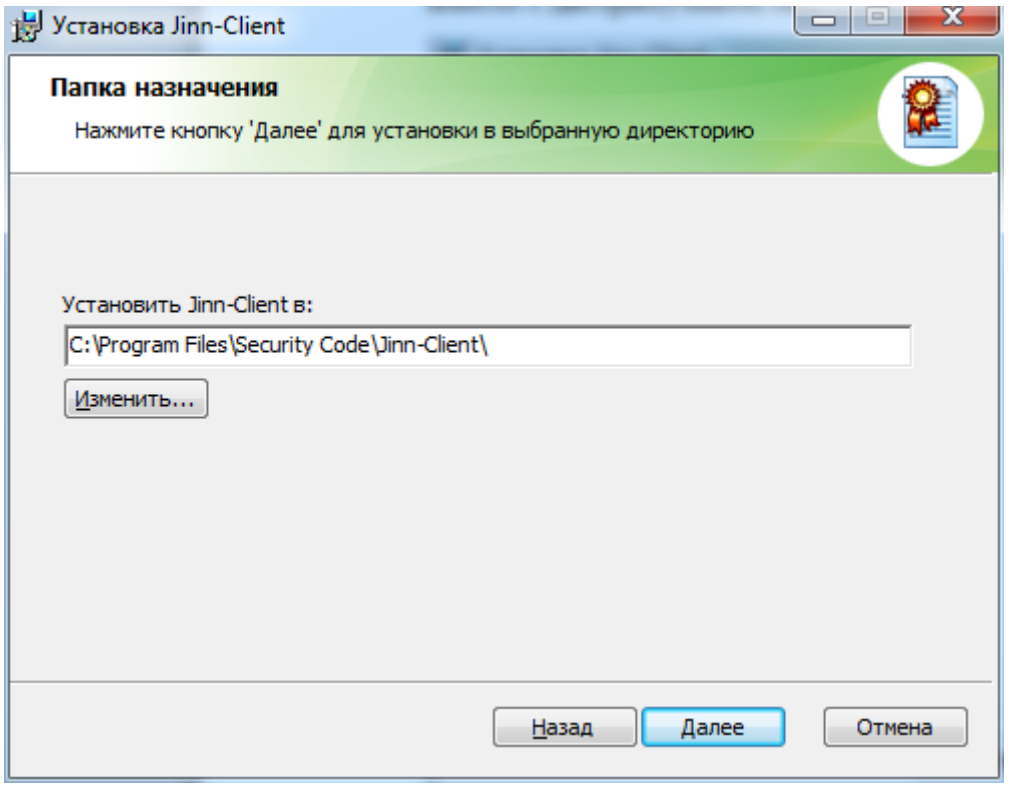


Рисунок 4.26. Окно выбора пути установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

65) Оставьте путь установки по умолчанию. Нажмите кнопку «Далее».

66) В диалоге настройки параметров СКЗИ «Программа доверенной визуализации подписи «Jinn-Client», ничего не изменяя, нажмите кнопку «Далее».

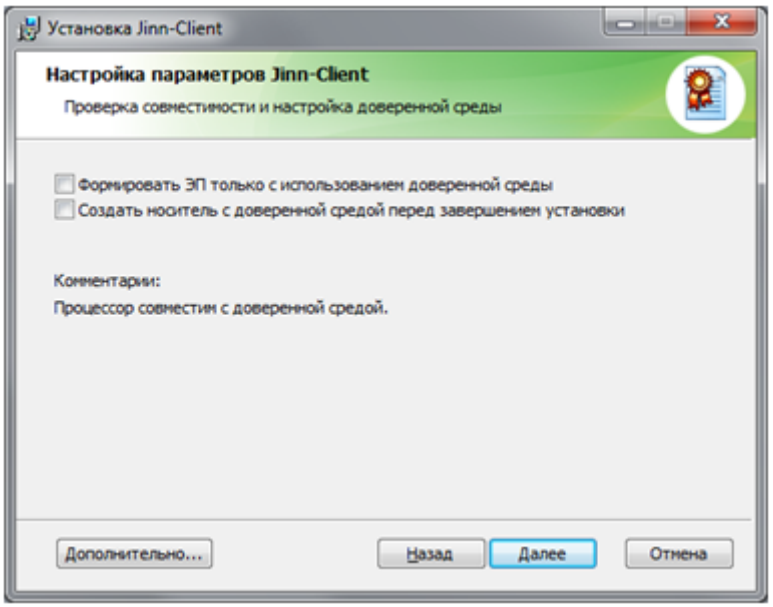


Рисунок 4.27. Окно настройки параметров СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

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

67) Далее пользователю будет выведено информационное сообщение о готовности к установке СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

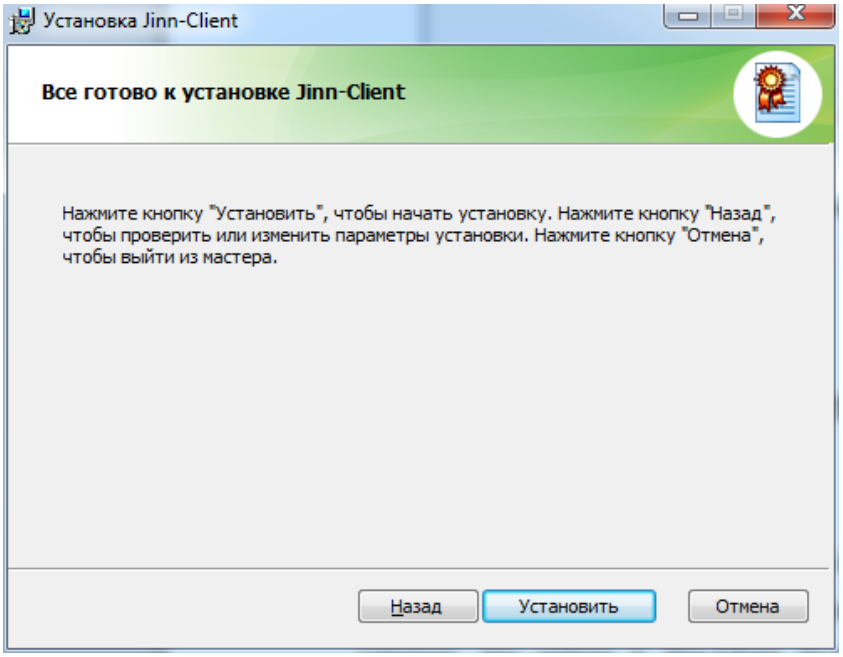


Рисунок 4.28. Сообщение о готовности к установке Jinn-Client

68) Нажмите кнопку «Установить». На экране отобразится диалог процесса установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

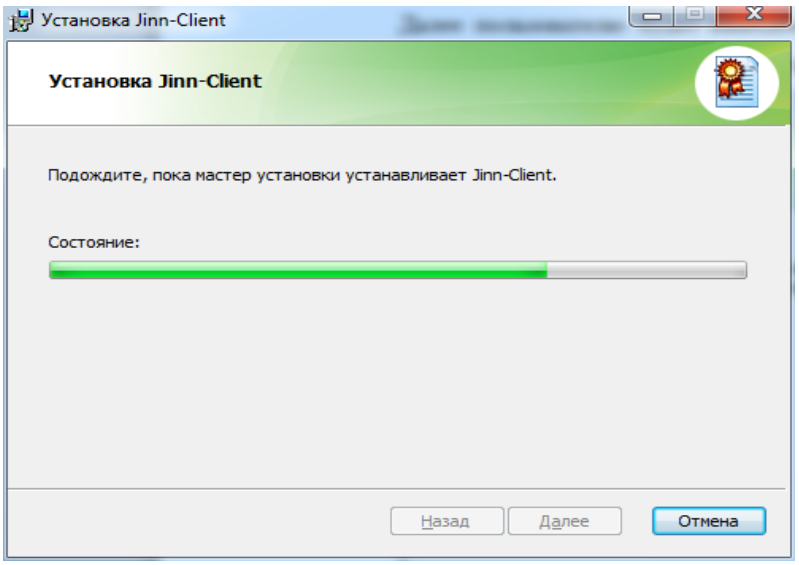


Рисунок 4.29. Окно, информирующее пользователя о прогрессе в процессе установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

69) По завершению установки на экран будет выведен диалог об успешном завершении установки.

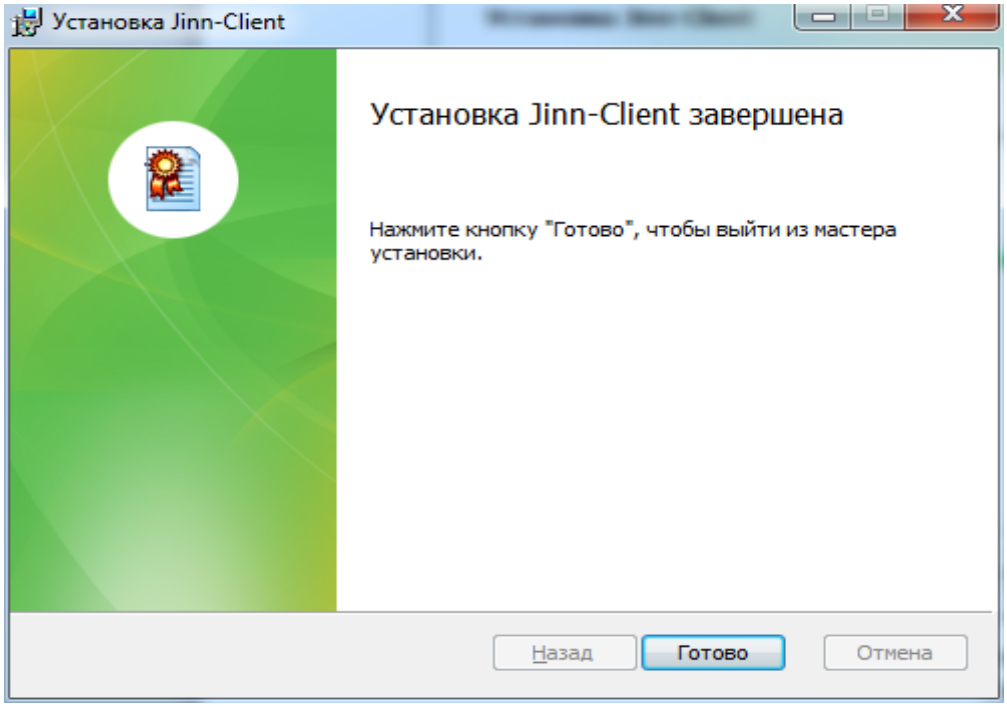


Рисунок 4.30. Сообщение об успешном завершении установки СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

70) Нажмите кнопку «Готово».

71) На предложение перезагрузки АРМ нажмите «Да».

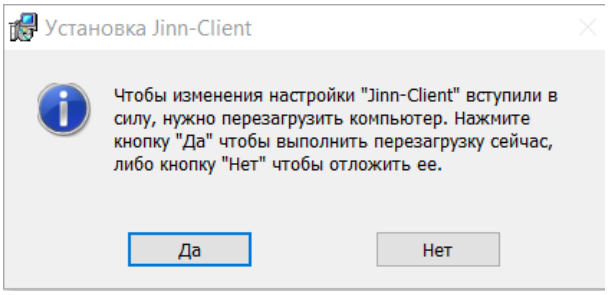


Рисунок 4.31. Сообщение о перезагрузке АРМ

4.8.2 Установка ПО «eXtended Container»

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

4.8.2.2 Установка XC должна производиться строго из дистрибутива Jinn-Client.

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

4.8.2.4 **Если на АРМ устанавливается Континент TLS Клиент, тогда установка XC должна производиться из дистрибутива Jinn-Client строго после установки Континент TLS Клиента с предварительным удалением dthcc eXtended Container 1.0.2.2 с перезагрузкой АРМ**.

4.8.2.5 Для установки ПО «eXtended Container» необходимо:

1) В АРМ пользователя вставить носитель информации, содержащий дистрибутив СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

72) В составе дистрибутива СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» осуществить запуск исполняемого файла «Setup.exe». На экране отобразится меню единого установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client».

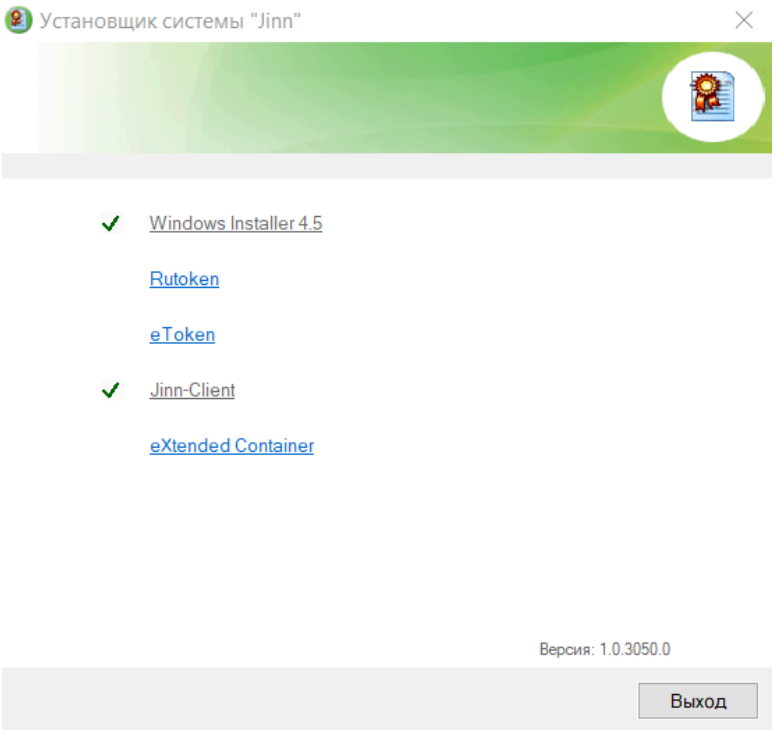


Рисунок 4.32. Меню единого установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client»

73) В меню установщика СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» активировать ссылку «eXtended Container». На экране отобразится меню мастера установки ПО «eXtended Container».

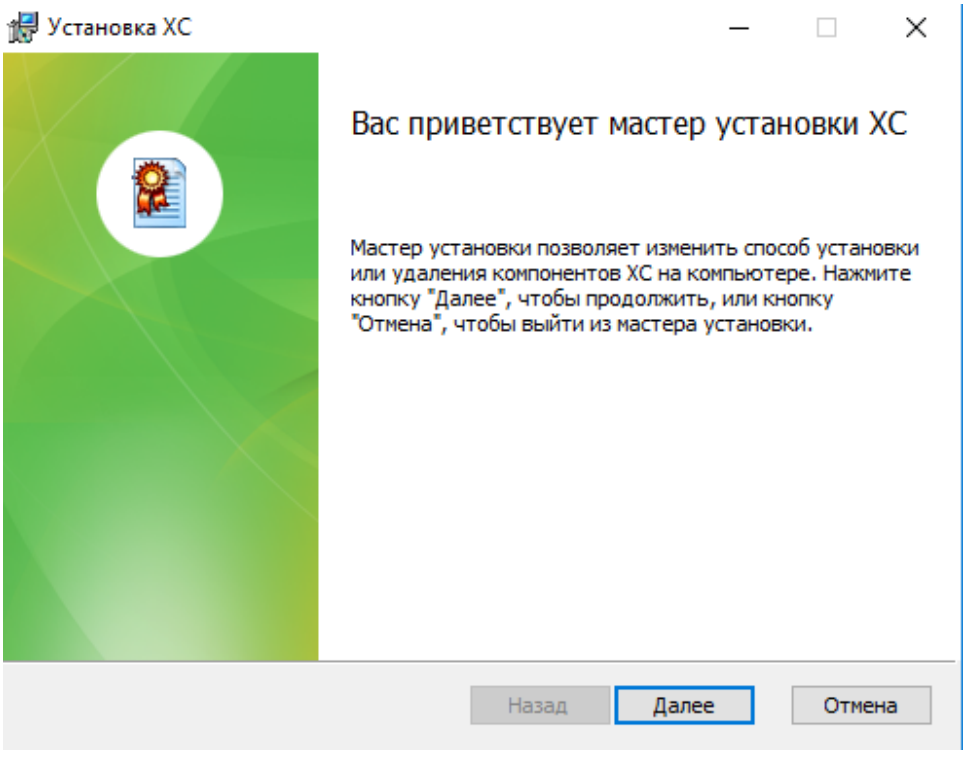


Рисунок 4.33. Окно приветствия установщика ПО «eXtended Container»

74) Для продолжения установки нажмите кнопку «Далее».

На экране отобразится диалог ввода лицензионного ключа, поставляемого вместе с дистрибутивом СКЗИ «Программа доверенной визуализации подписи «Jinn-Client» в электронном или бумажном виде.

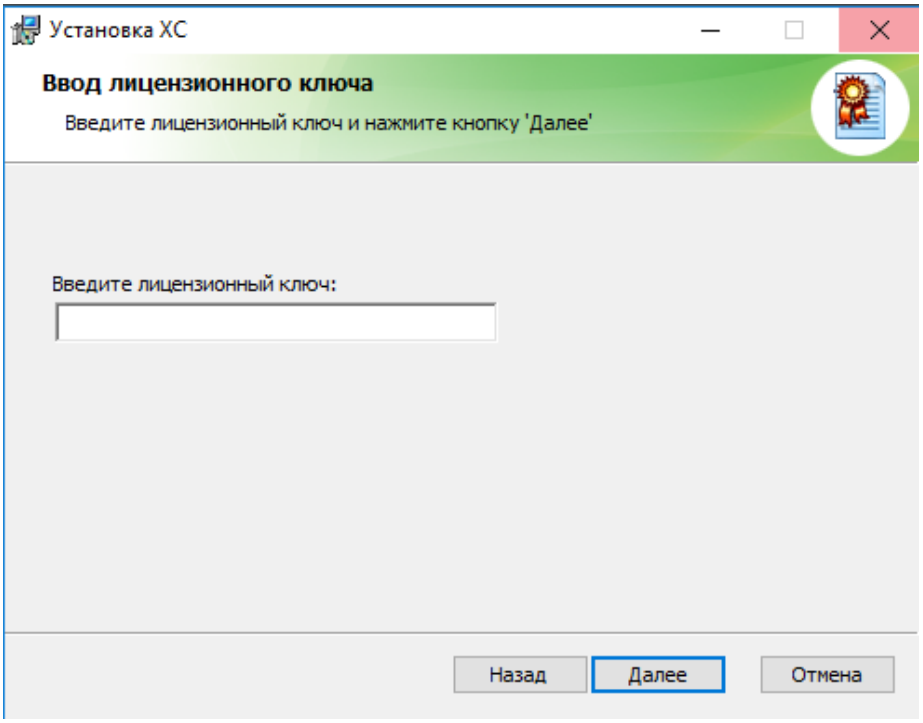


Рисунок 4.34. Окно ввода лицензионного ключа

75) Введите лицензионный ключ и нажмите кнопку «Далее». Пользователю будет выведено информационное сообщение о готовности к установке ПО «eXtended Container».

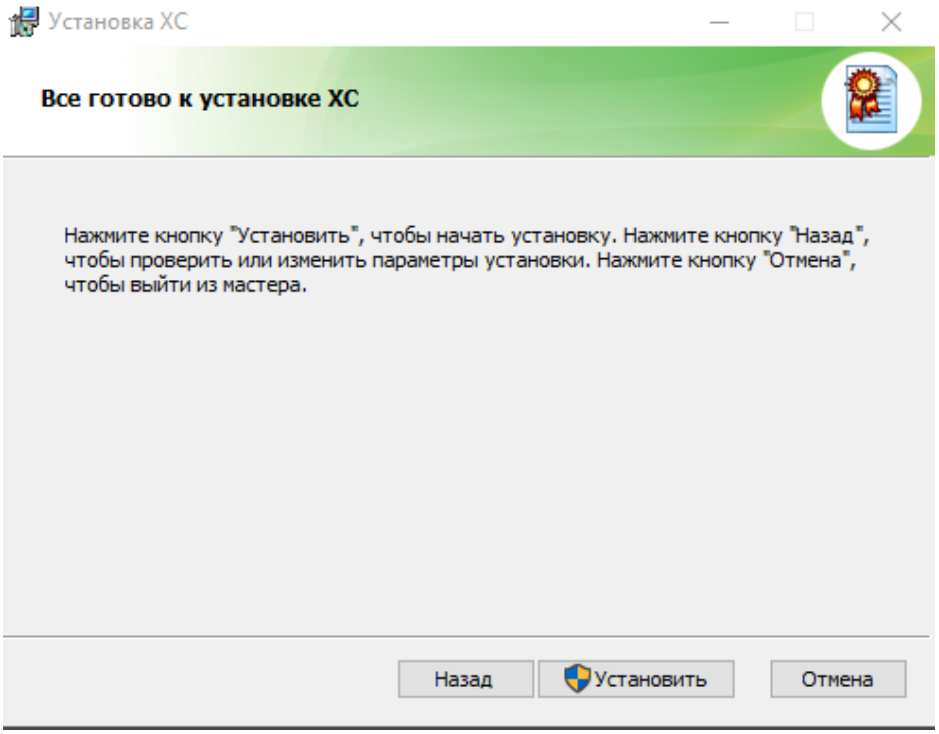


Рисунок 4.35. Сообщение о готовности к установке "eXtended Container"

76) Нажмите кнопку «Установить». На экране отобразится диалог процесса установки ПО «eXtended Container».

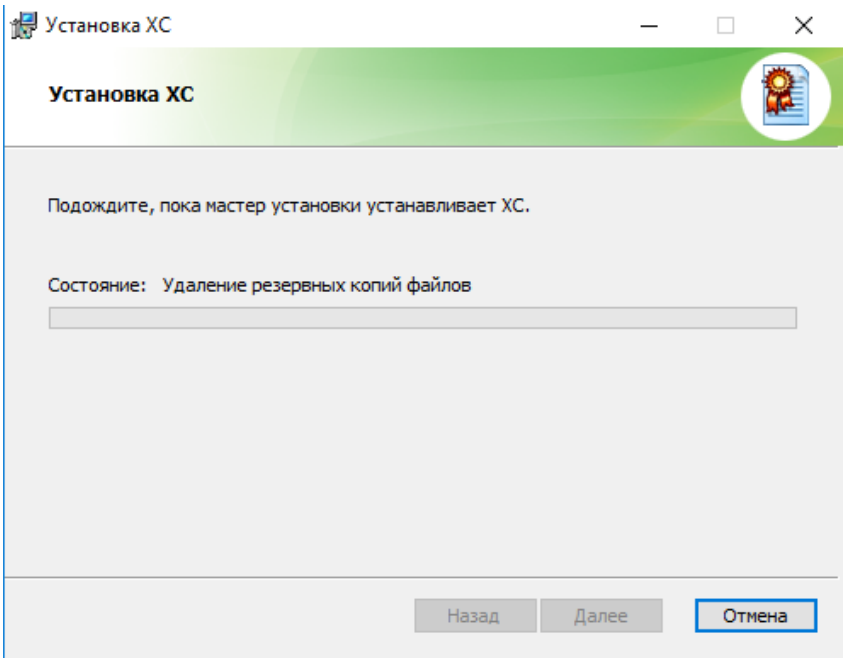


Рисунок 4.36. Окно, информирующее пользователя о прогрессе установки ПО «eXtended Container»

77) По завершению установки на экран будет выведен диалог об успешном завершении установки.

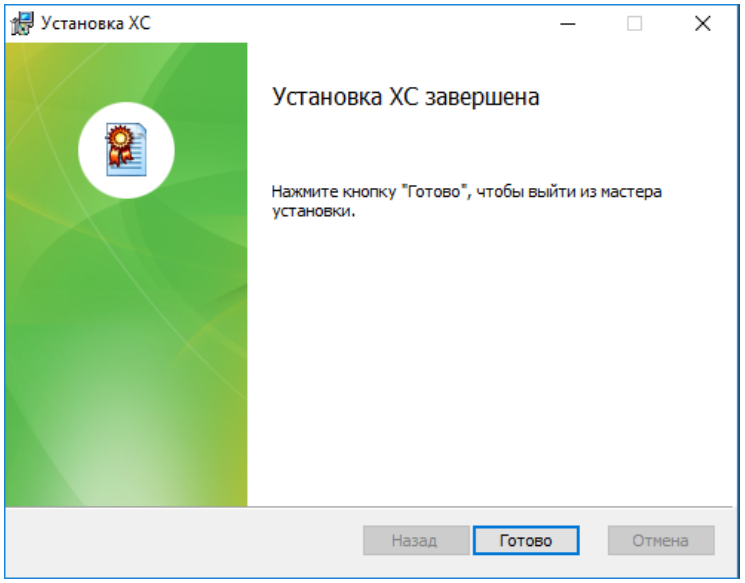


Рисунок 4.37. Сообщение об успешном завершении установки ПО «eXtended Container»

78) Нажмите кнопку «Готово». После установки ПО «eXtended Container» необходимо осуществить перезагрузку АРМ.

4.9 Установка сертификата пользователя, созданного в Код Безопасности CSP (при необходимости)

Ели сертификат пользователя создан с использованием Код Безопасности CSP, тогда необходимо выполнить следующие действия:

1) Запустить «Код Безопасности CSP»

79) Перейти на вкладку «Ключевые контейнеры» и проверить доступность необходимых контейнеров.

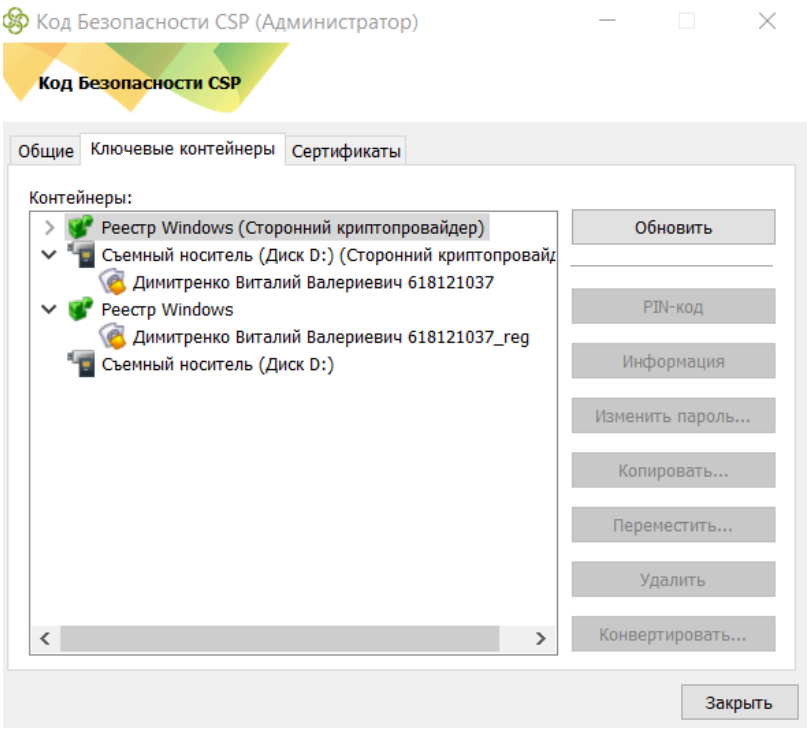


Рисунок 4.38. Доступные ключевые контейнеры

80) Перейти на вкладку «Сертификаты» и выбрать «Установить сертификат».

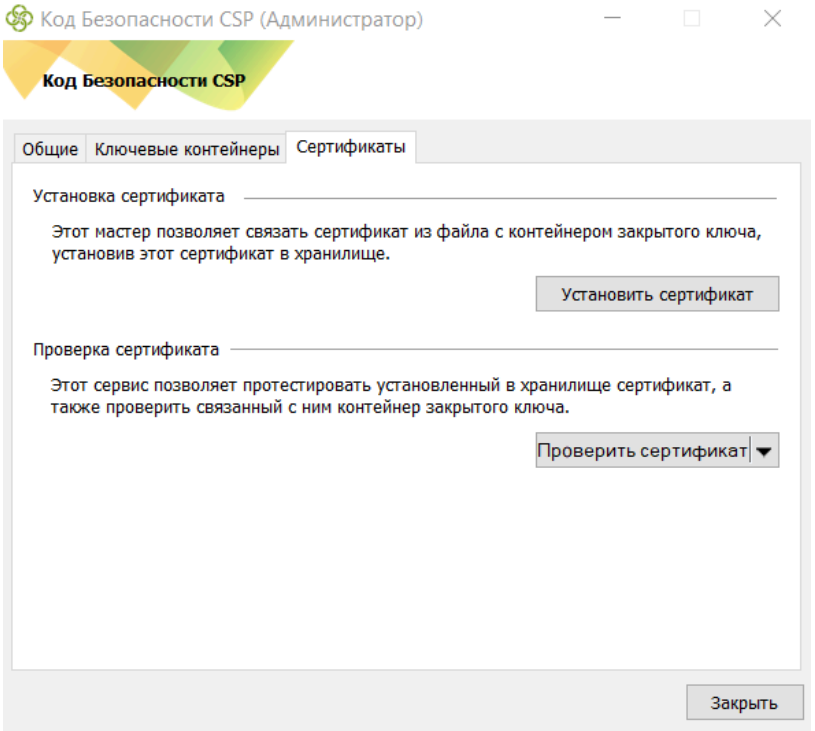


Рисунок 4.39. Вкладка «Сертификаты». Код Безопасности CSP.

81) В появившемся окне нажать на кнопку «Обзор…» и выбрать необходимый сертификат и нажать «Далее».

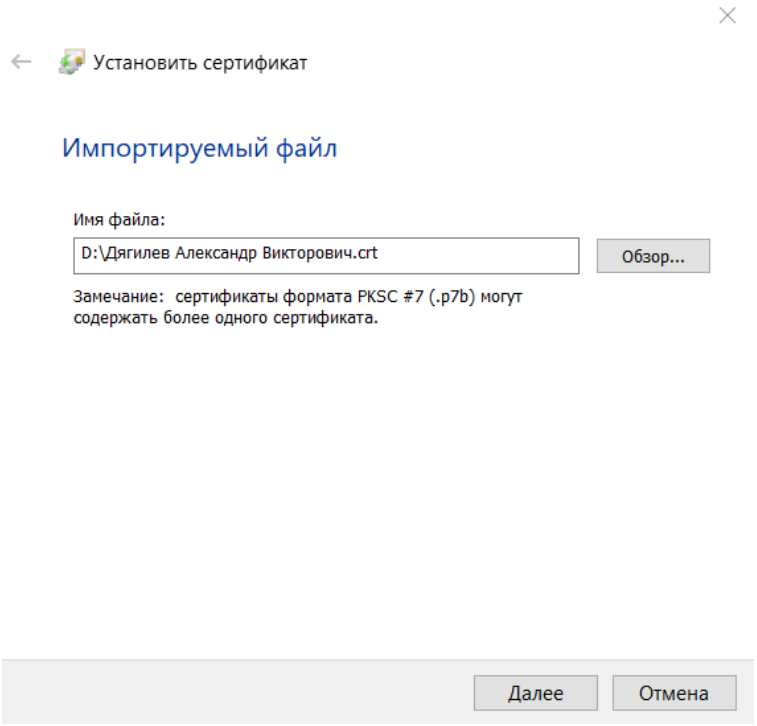


Рисунок 4.40. Выбрать сертификат для установки

82) В появившемся окне указать «Моей учетной записи пользователя» и «Личное». Выбрать необходимый сертификат и нажать «Далее».

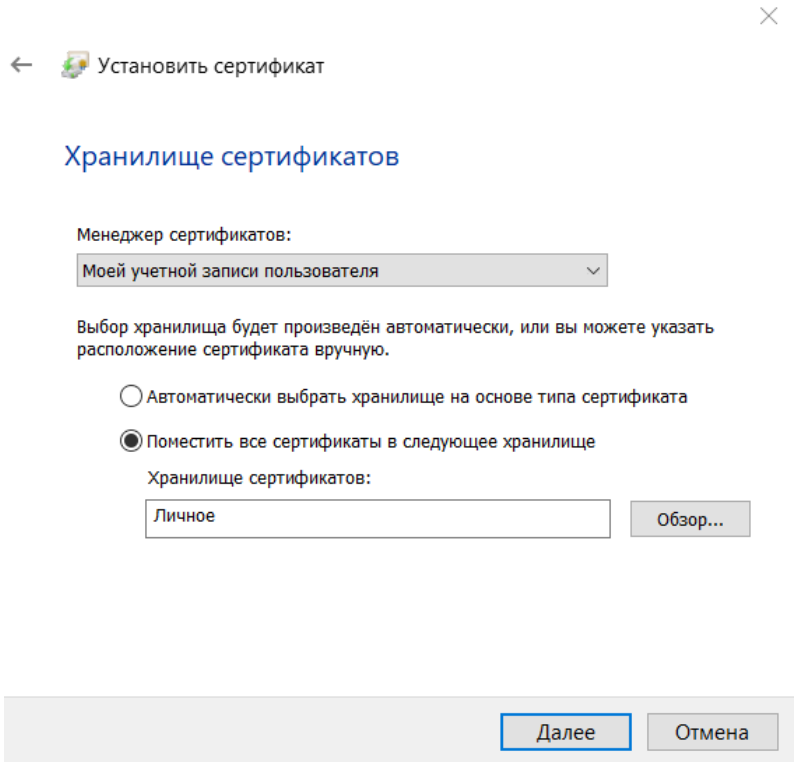


Рисунок 4.41. Выбор сертификата для установки

83) В появившемся окне выбрать соответствующий контейнер закрытого ключа сертификата и нажать «Далее».

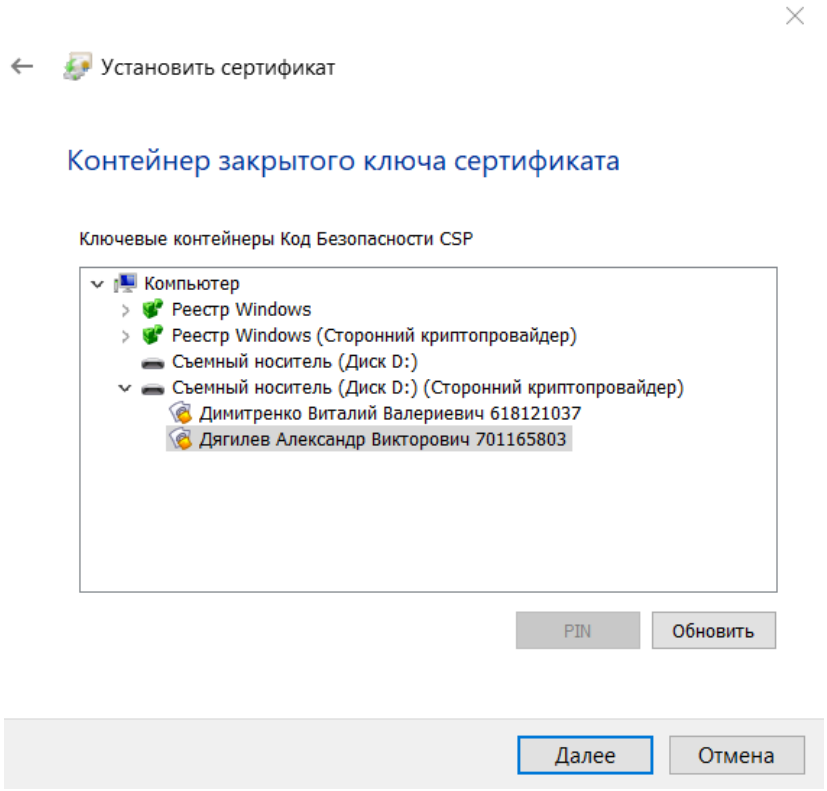


Рисунок 4.42. Выбор контейнера закрытого ключа

84) В открывшемся окне нажать «Готово».

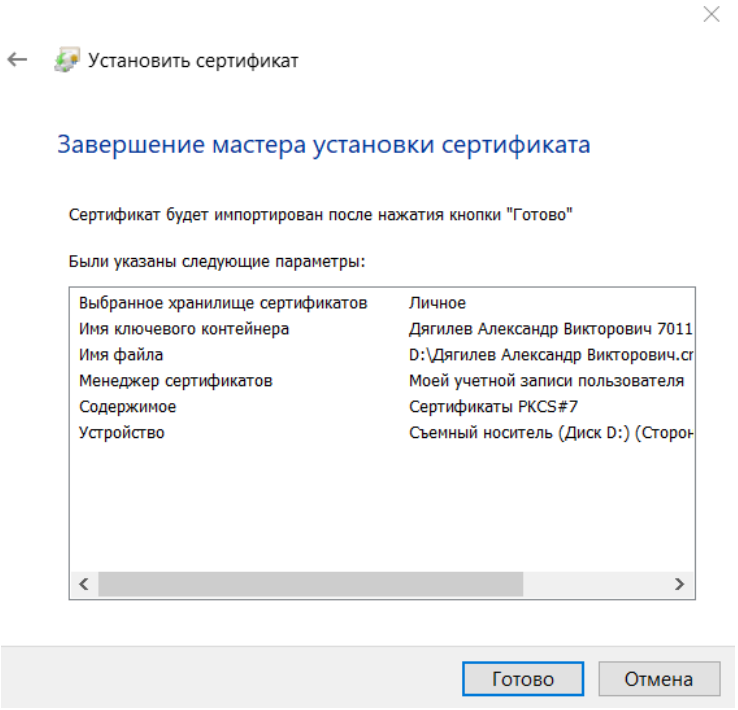


Рисунок 4.43. Завершение мастера установки сертификата

85) Указать пароль от контейнера закрытого ключа и нажать «Ок».

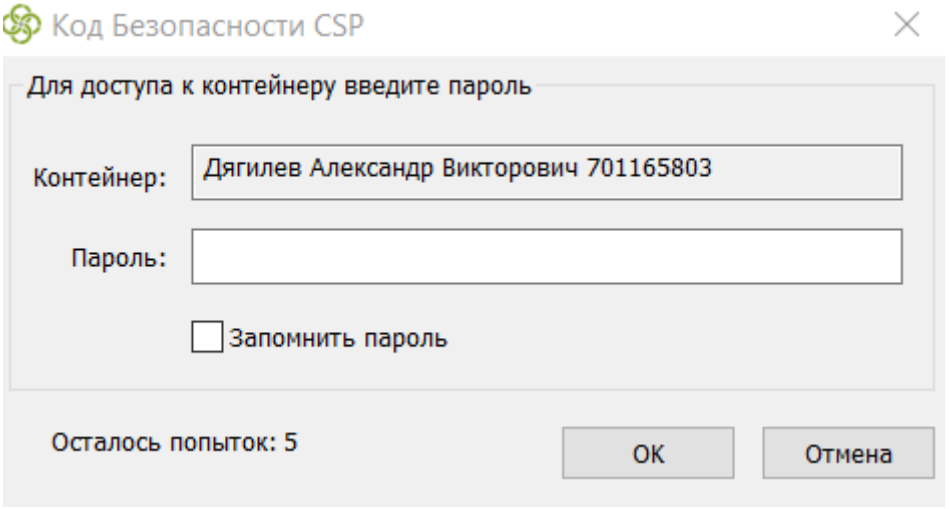


Рисунок 4.44. Выбор закрытого ключа

86) Успешность установки сертификата должно закончится сообщением. Нажать «Ок».

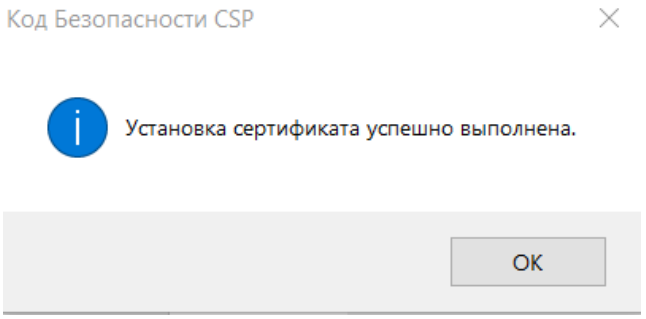


Рисунок 4.45. Выбор закрытого ключа

4.10 Настройка СКЗИ «Континент TLS VPN Клиент»

4.10.1Запустить СКЗИ «Континент TLS VPN Клиент», нажав на соответствующий ярлык на рабочем столе. В открывшемся окне нажать на кнопку «Добавить». Выбрать тип соединения «Ресурс»:

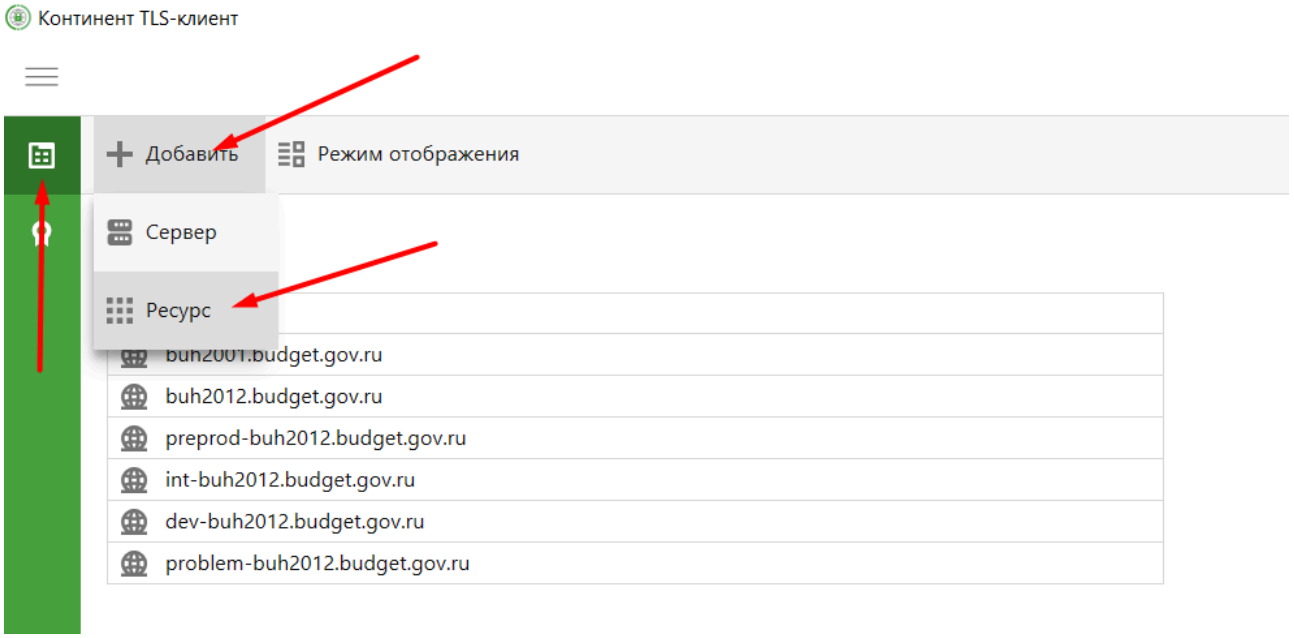


Рисунок 4.46. Вкладка «Главная». Континент TLS Клиент

4.10.2В окне добавления ресурса прописать следующие параметры.

Точка входа в Личный кабинет Электронного бюджета по сертификатам пользователей на основе ГОСТ Р 34.10-2012:

Адрес: buh2012.budget.gov.ru.
Имя ресурса: buh2012.budget.gov.ru.
Удаленный порт: 443
Тип: Прокси

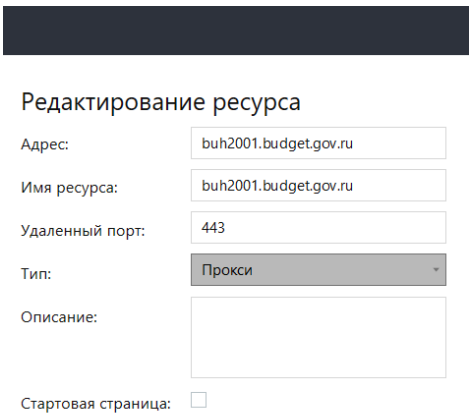


Рисунок 4.47. Редактирование ресурса

4.10.3 После введения параметров нажать кнопку «Сохранить».

4.10.4 Перейти во вкладку «Настройки». Выбрать раздел «Основные».

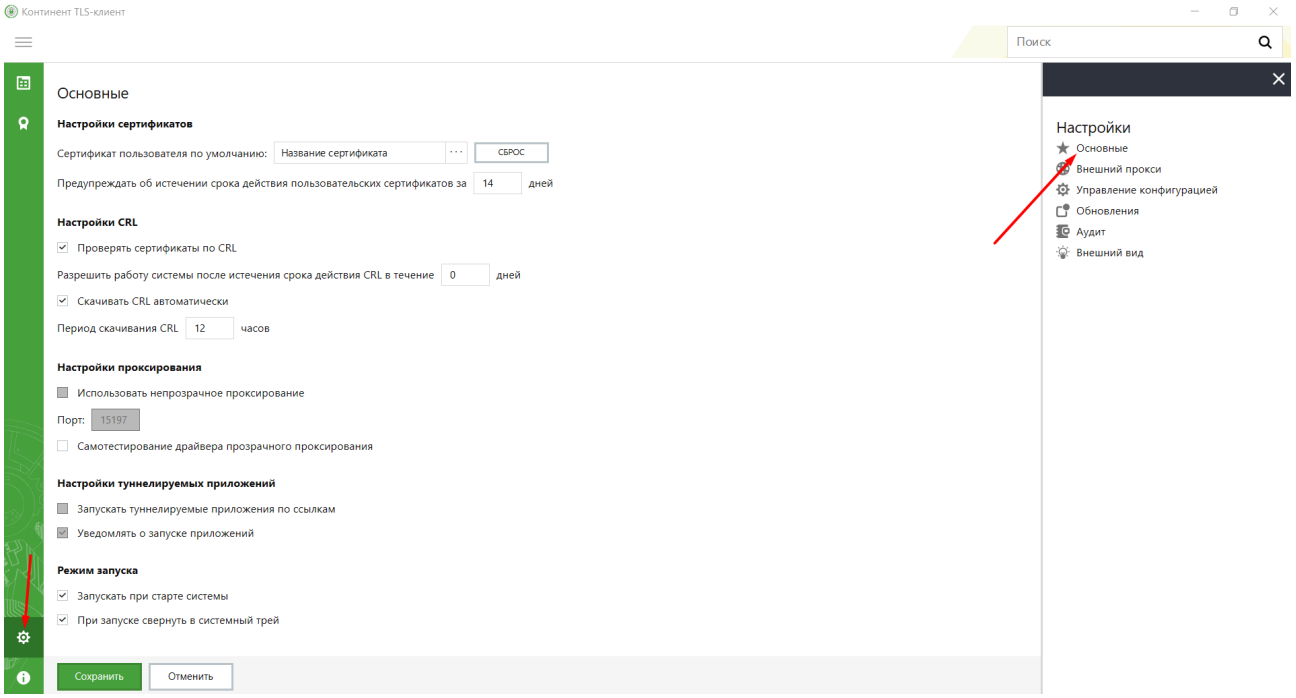


Рисунок 4.48. Раздел «Основные» вкладки «Настройки»

1) Необходимо отметить следующие чекбоксы:
   a) Проверять сертификаты по CRL.
s) Скачивать CRL автоматически.
t) Запускать при старте системы.
u) При запуске свернуть в системный трей.
87) Нажать кнопку «Сохранить».

4.10.5 Перейти в раздел «Внешний прокси».

1) Отметить чекбокс «Настраивать автоматически».

a) В случае, если в организации используется прокси-сервер, после сохранения настроек его параметры определятся автоматически.

b) Если прокси-сервер не используется, после сохранения окно параметров останется пустым.

Окно настроек внешнего прокси должно выглядеть следующим образом:

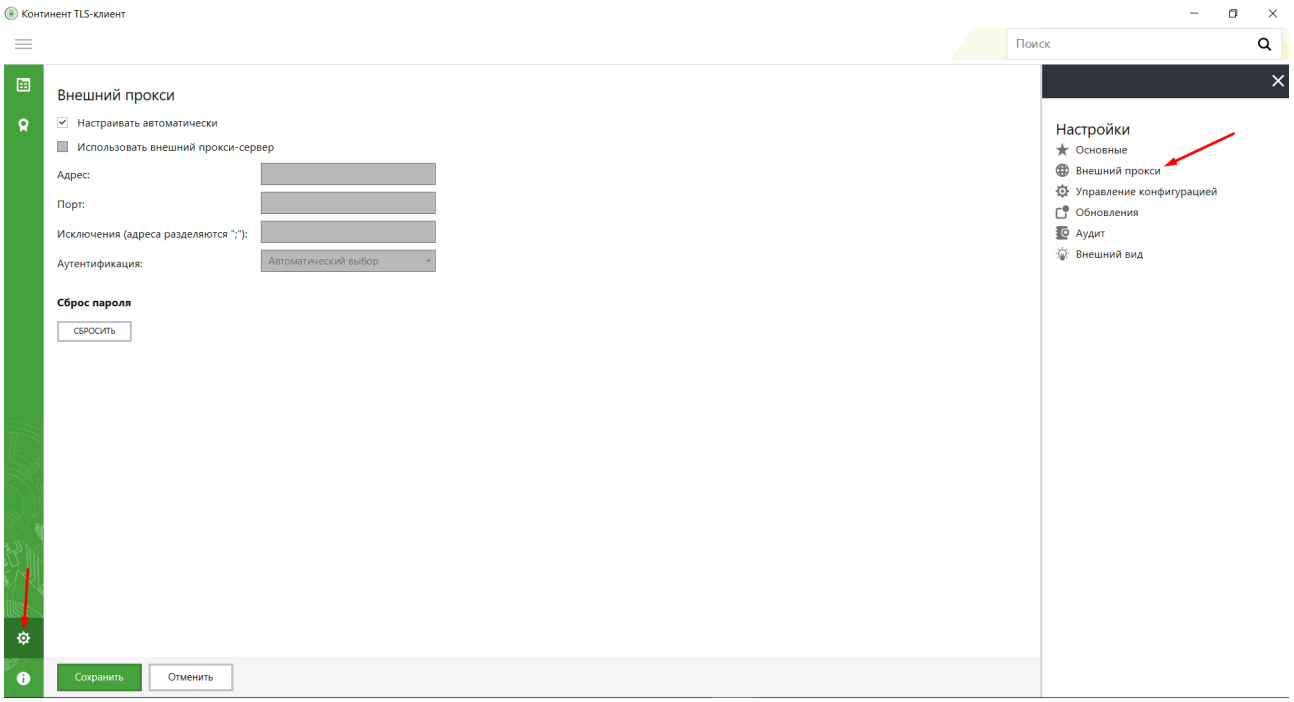


Рисунок 4.49. Вкладка «Настройки». Раздел «Внешний прокси». Континент TLS Клиент

4.10.6Перейти во вкладку «Управление сертификатами». Выбрать раздел «Серверные сертификаты».

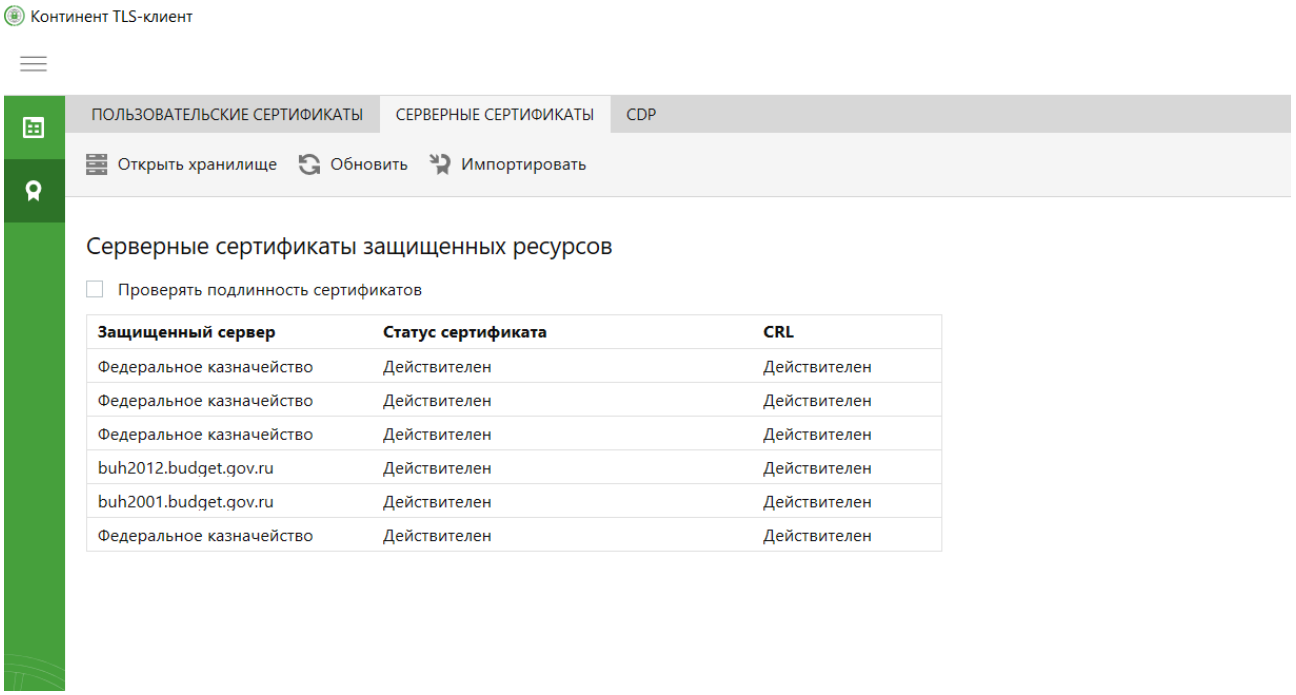


Рисунок 4.50. Вкладка «Управление сертификатами»

4.10.7Выбрать из списка просроченные сертификаты и удалить их по очереди.

4.10.8Нажать на кнопку «Импортировать». В открывшемся меню выбрать необходимый сертификат сервера в зависимости от используемой точки входа.

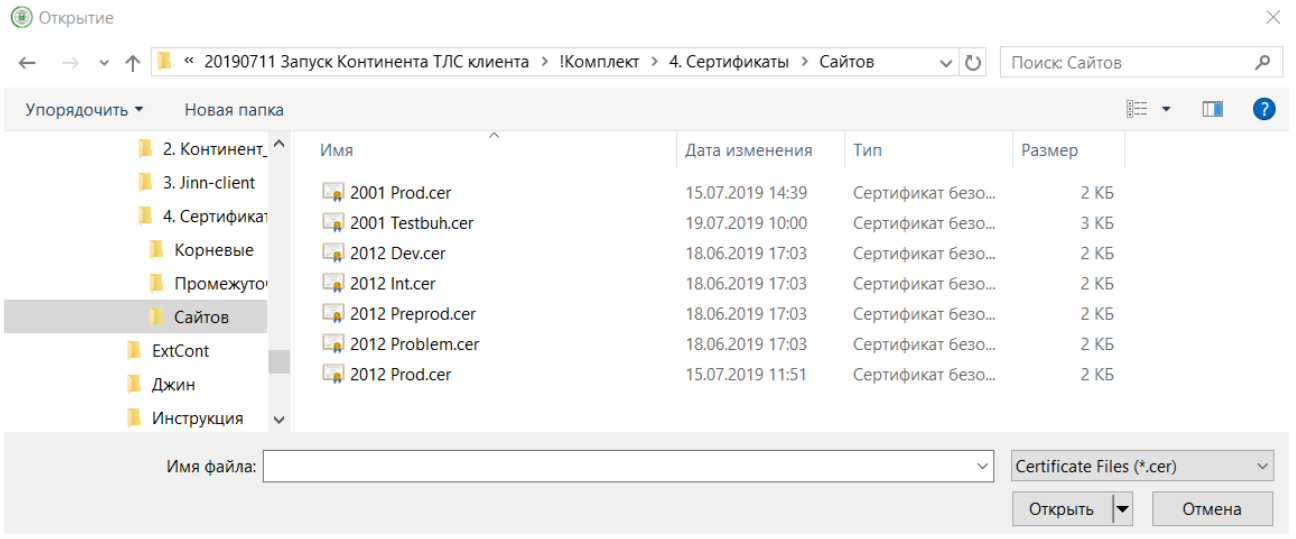


Рисунок 4.51. Выбор серверного сертификата

4.10.9Перейти в раздел CDP и нажать кнопку «Скачать CRL».

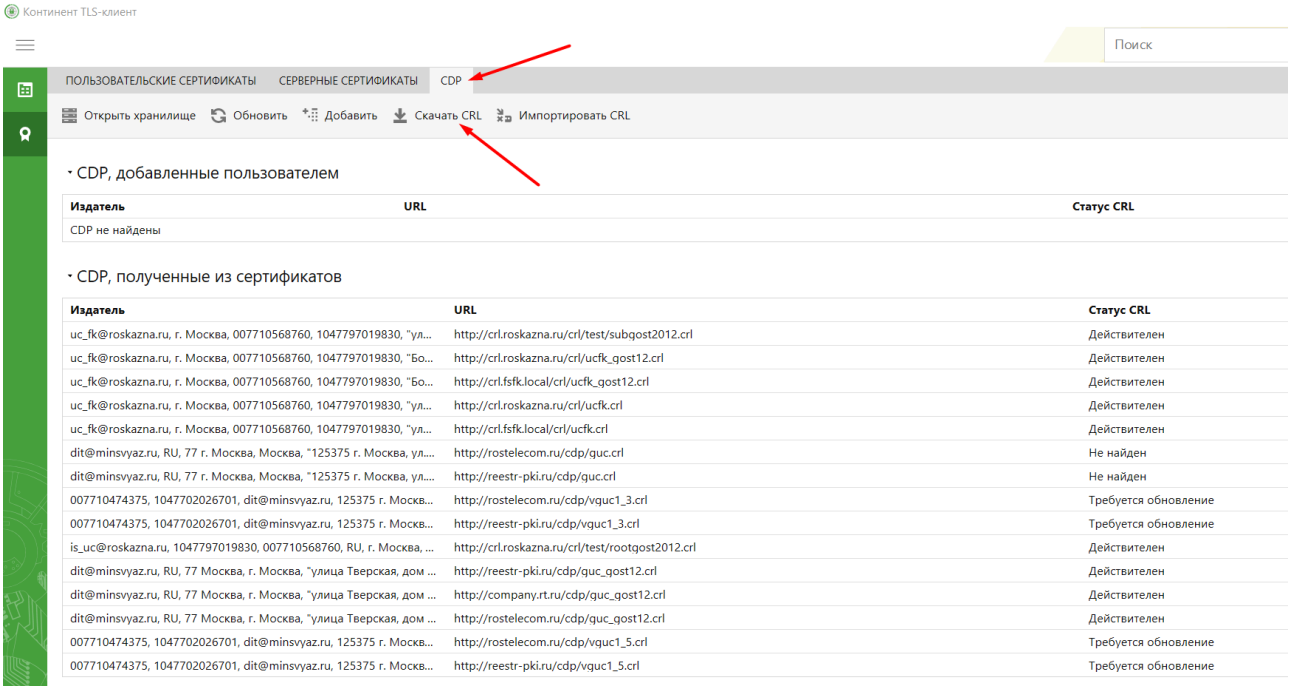


Рисунок 4.52. Окно CDP. Континент TLS Клиент

4.10.10 Перейти во вкладку «Управление сертификатами». Выбрать раздел «Серверные сертификаты». Нажать «Обновить».

4.10.11 У установленных сертификатов должен стоять Статус сертификата «Действителен», в колонке CRL также должен стоять статус «Действителен».

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

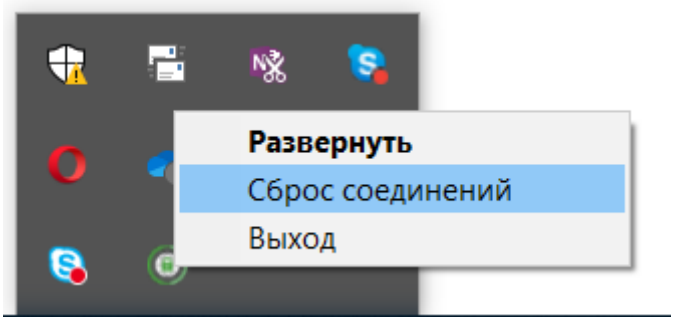


Рисунок 4.53. Сброс соединений

4.11 Настройка подписания ЭП для веб-обозревателей, отличных от Internet Explorer

4.11.1 Установка Jinn Sign Extension Provider

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

4.11.1.2 В случае отсутствия дистрибутива необходимо обратиться в ОРСиБИ Федерального казначейства своего региона.

4.11.1.3 Рекомендуемая сборка Jinn Sign Extension Provider 1.1.0.5.

4.11.1.4 Для установки Jinn Sign Extension Provider необходимо:

1) Запустить файл установки. Откроется окно приветствия:

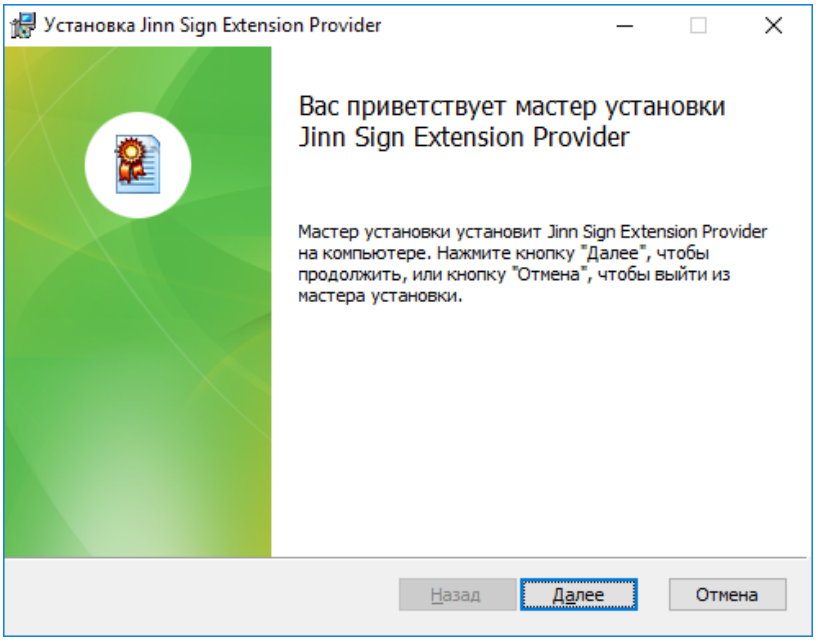


Рисунок 4.54. Приветственное окно установки Jinn Sign Extension Provider

88) Нажать кнопку «Далее». Откроется окно «Лицензионного соглашения». Отметить чекбокс «Я принимаю условия лицензионного соглашения».

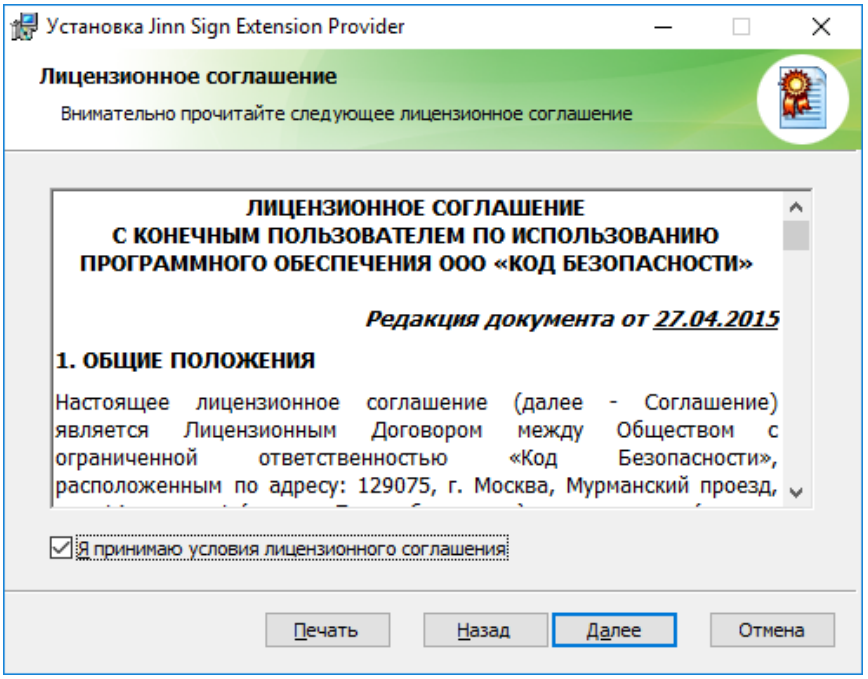


Рисунок 4.55. Окно лицензионного соглашения Jinn Sign Extension Provider

89) Нажать кнопку «Далее». Откроется окно пути установки.

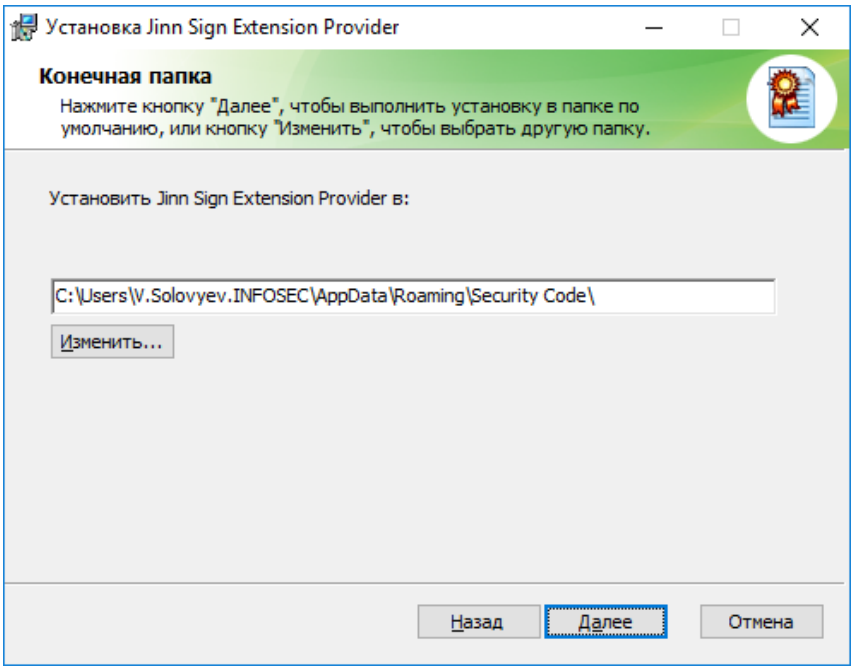


Рисунок 4.56. Окно пути установки Jinn Sign Extension Provider

90) Нажать кнопку «Далее». Откроется окно установки.

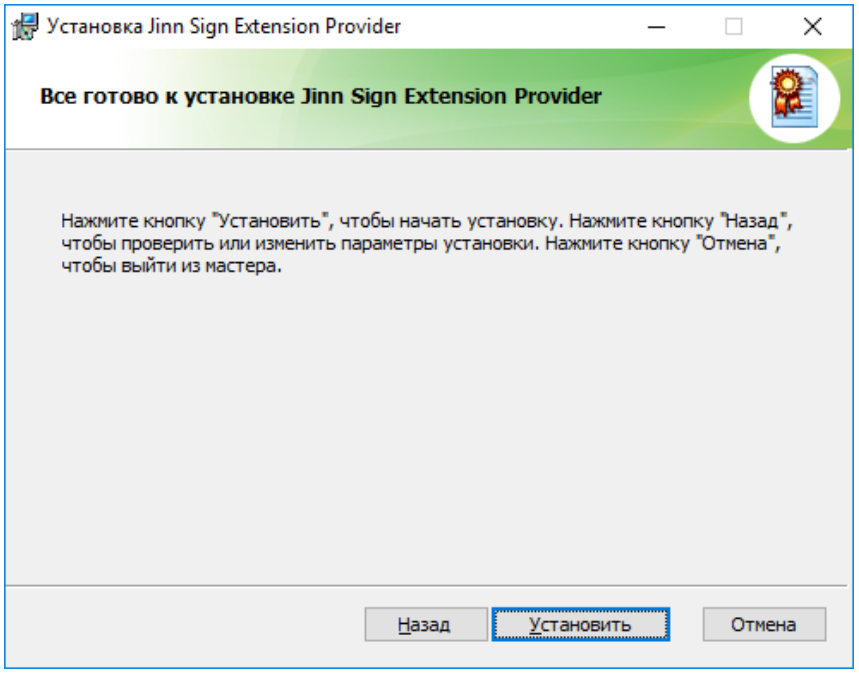


Рисунок 4.57. Окно установки Jinn Sign Extension Provider

91) Нажать кнопку «Установить». Произведется установка провайдера и появится окно завершения установки.

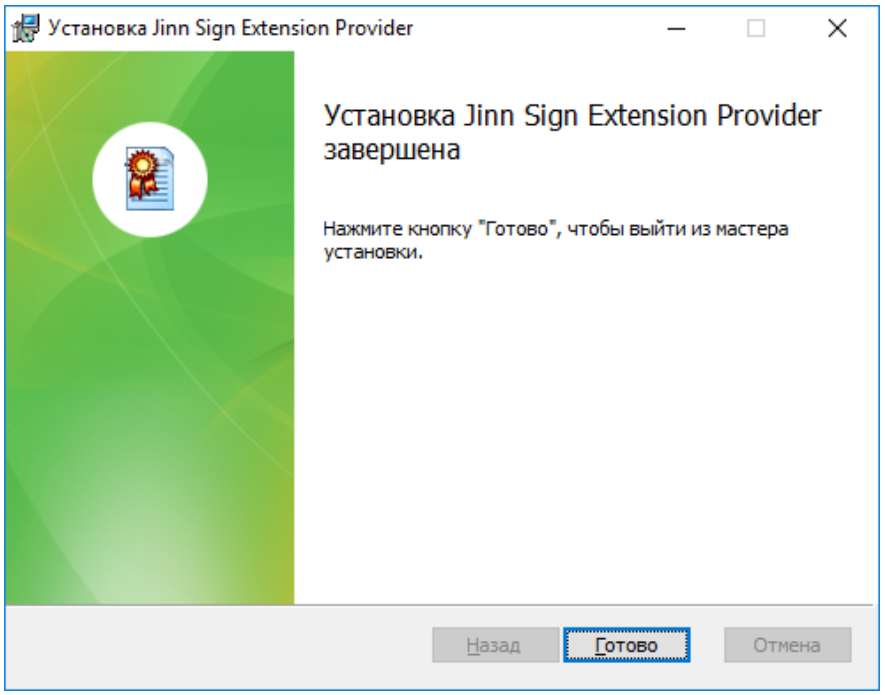


Рисунок 4.58. Окно завершения установки Jinn Sign Extension Provider

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

93) Перезагрузите АРМ.

4.11.2 Установка расширения Jinn Sign Extension

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

4.11.2.1 Google Chrome

4.11.2.1.1 Установка расширения для АРМ в Интернет

Установка расширения Jinn Sign Extension 1.2.0.1 для браузера Google Chrome осуществляется через интернет-магазин chrome (доступен по ссылке из сети Интернет https://chrome.google.com/webstore/category/extensions) .

Необходимо:

1) Открыть магазин Google Chrome.

94) Выполнить поиск по ключевым словам Jinn Sign Extension. Среди результатов поиска выбрать расширение Jinn Sign Extension.

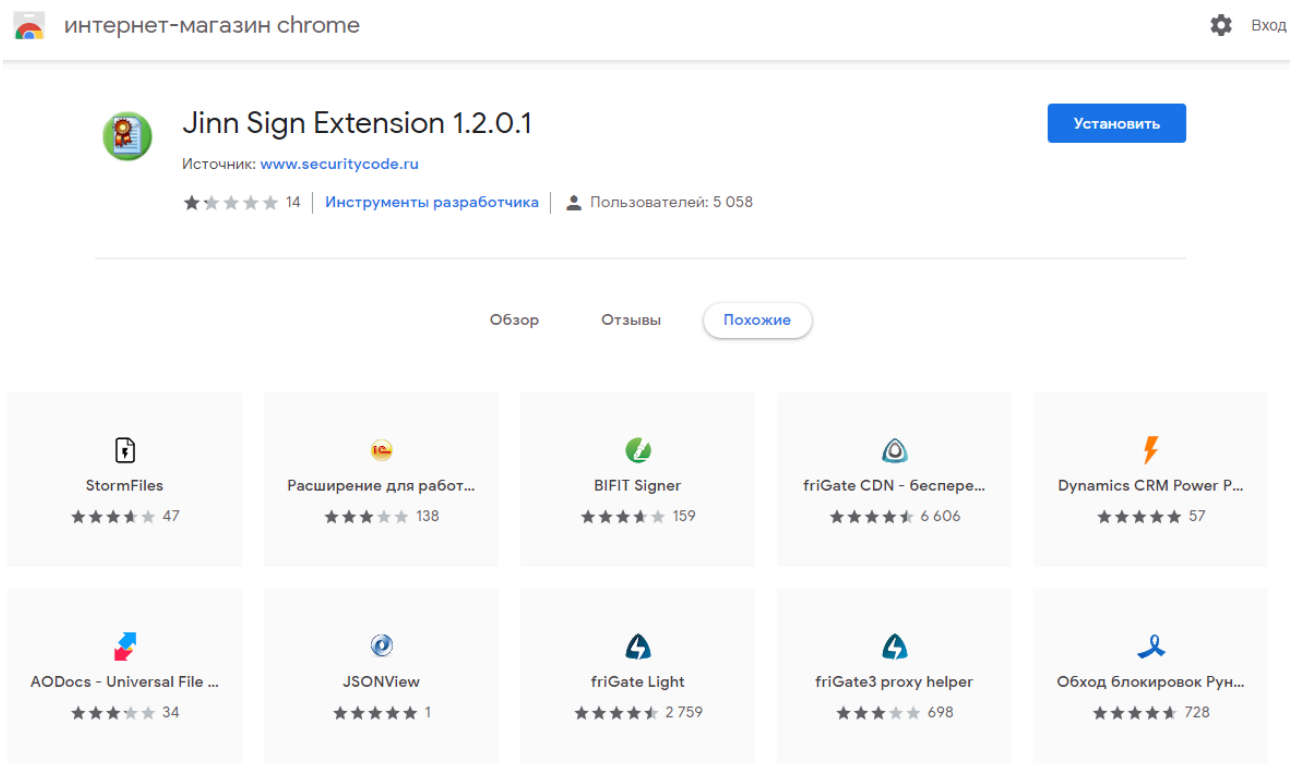


Рисунок 4.59. Страница Jinn Sign Extension в интернете-магазине chrome

95) Нажать кнопку «Установить». При этом пользователю будет предложено подтвердить установку данного расширения.

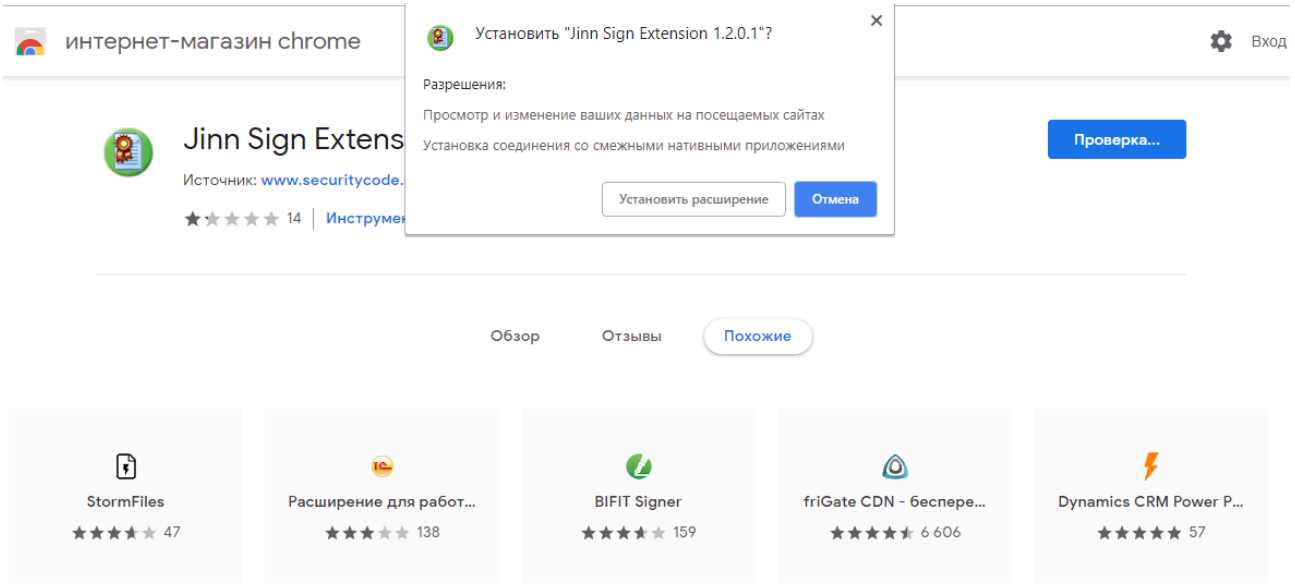


Рисунок 4.60. Окно с подтверждением установки расширения Jinn Sign Extension

96) Нажать кнопку «Установить расширение». Об успешной установке расширения Jinn Sign Extension будет свидетельствовать появившееся окно с соответствующим сообщением в правом верхнем углу браузера.

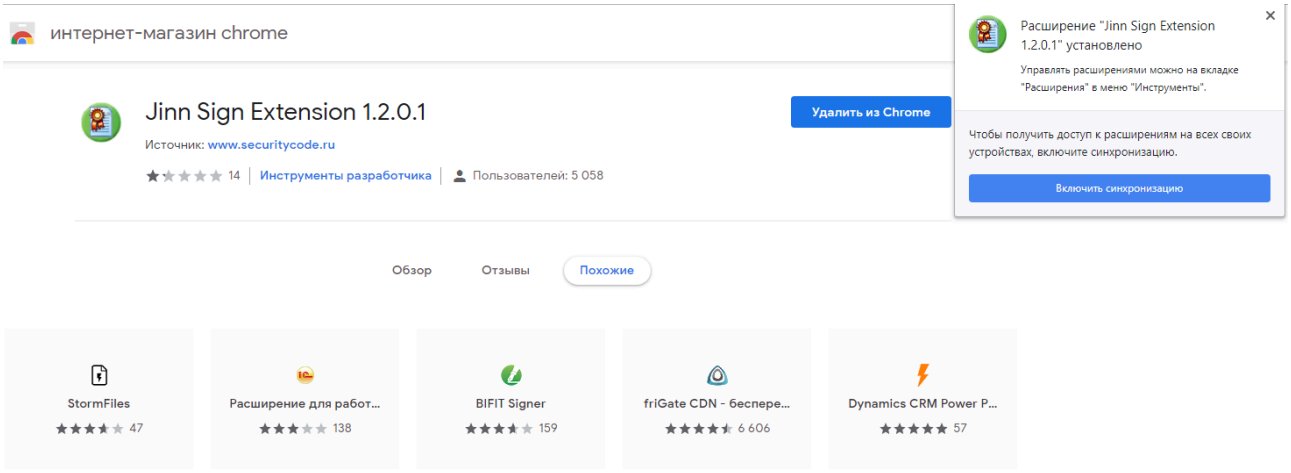


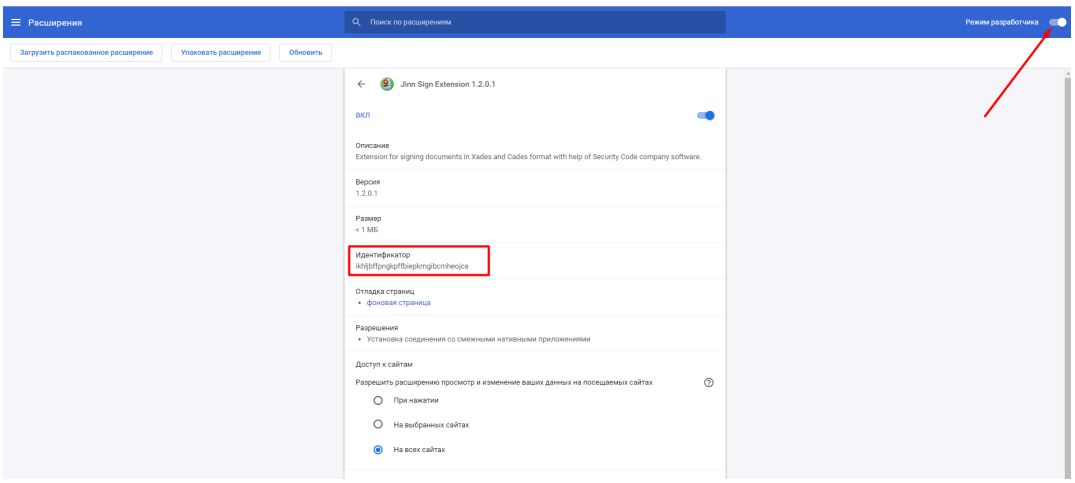
Рисунок 4.61. Сообщение об успешном завершении установки расширения Jinn Sign Extension

97) Закрыть окно с сообщением об успешной установке.

4.11.2.1.2 Установка расширения для АРМ в ЗКВС

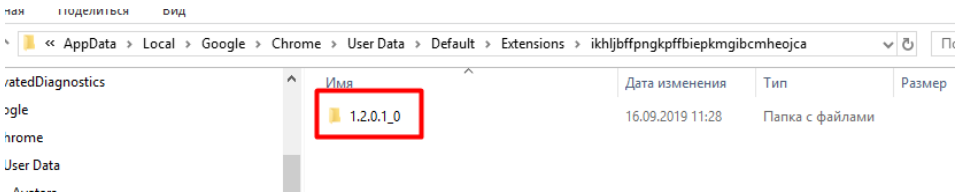
Предварительно необходимо на АРМ в Интернете сформировать распакованный пакет с расширением Jinn Sign Extension.

1) На АРМ в Интернете откройте раздел Chrome с расширениями chrome://extensions/, выберете расширение Jinn Sign Extension и включите режим разработчика.



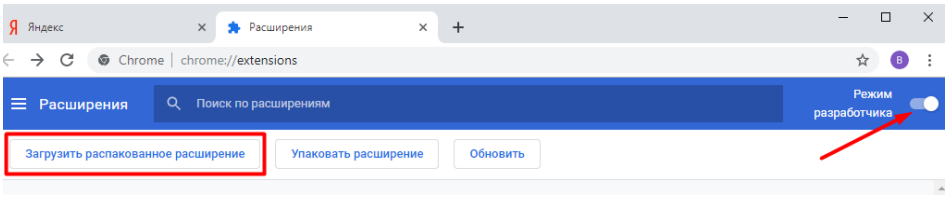
98) Откройте папку в Проводнике C:\Users\%Имя пользователя%\AppData\Local\Google\Chrome\User Data\Default\Extensions\%Идентификатор расширения%\

99) Сохраните папку 1.2.0.1_0 на флешку для переноса на АРМ в ЗКВС

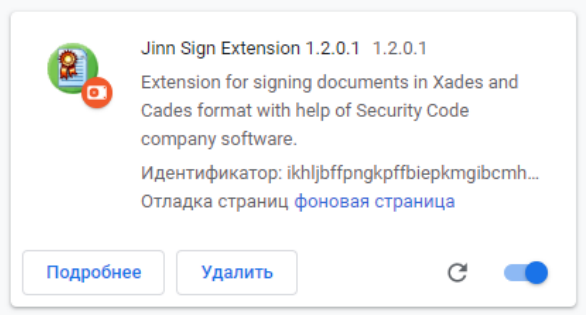


100) Перенесите данную папку на АРМ в ЗКВС.

101) Откройте на АРМ в ЗКВС раздел Chrome с расширениями chrome://extensions/, включите режим разработчика и нажмите «Загрузить распакованное расширение»:



102) В разделе расширения появится установленное расширение:



103) Отключите режим разработчика.

4.11.2.1.3 Настройка расширения

1) Открыть окно настройки расширений из пункта меню «Дополнительные инструменты»:

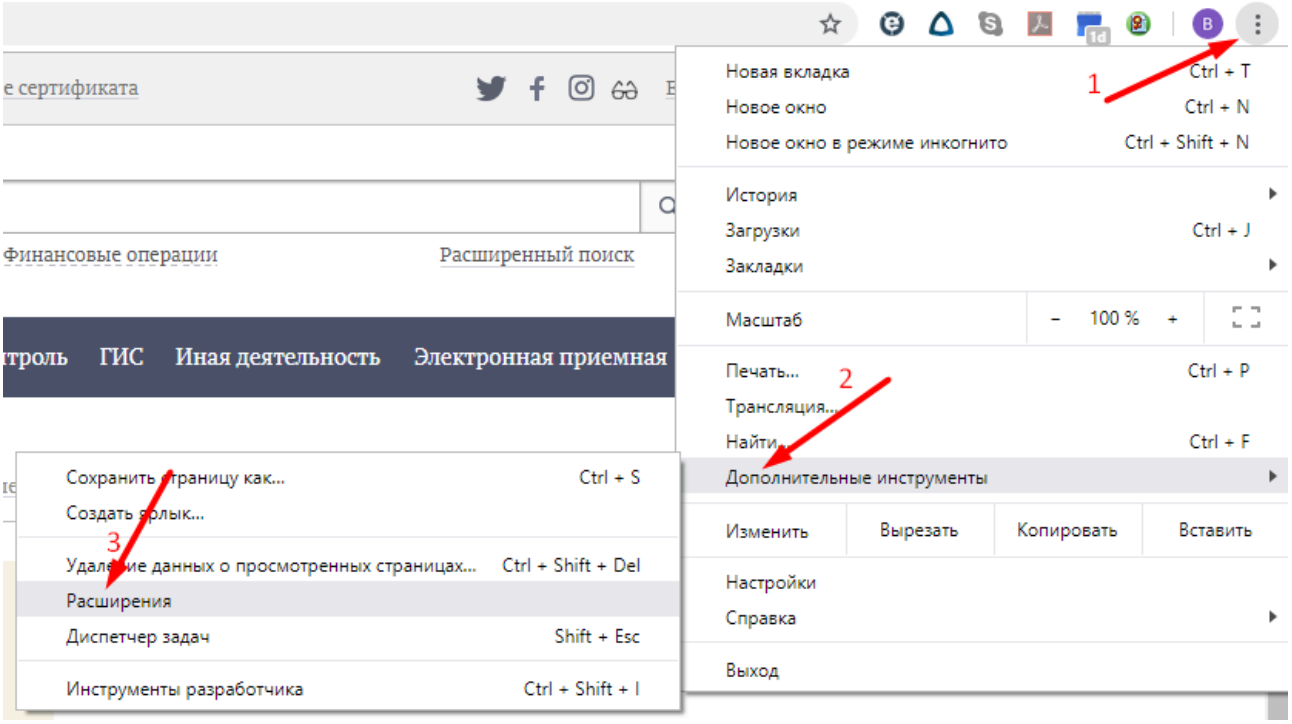


Рисунок 4.62. Расширения Chrome

104) Для расширения «Jinn Sign Extension» нажать «Подробнее»

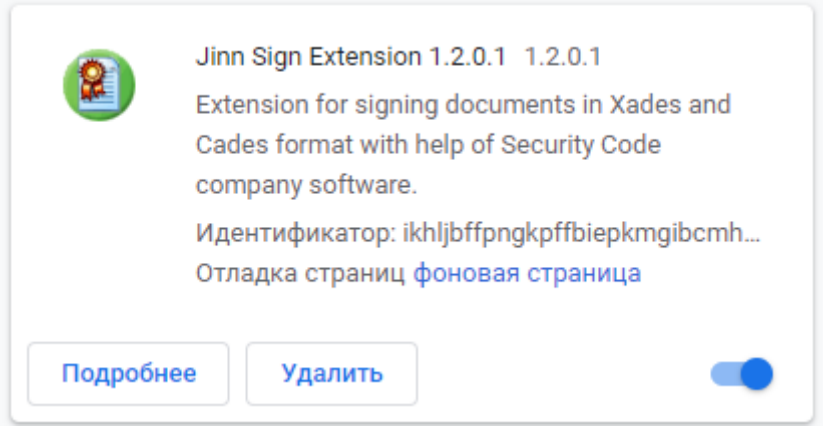
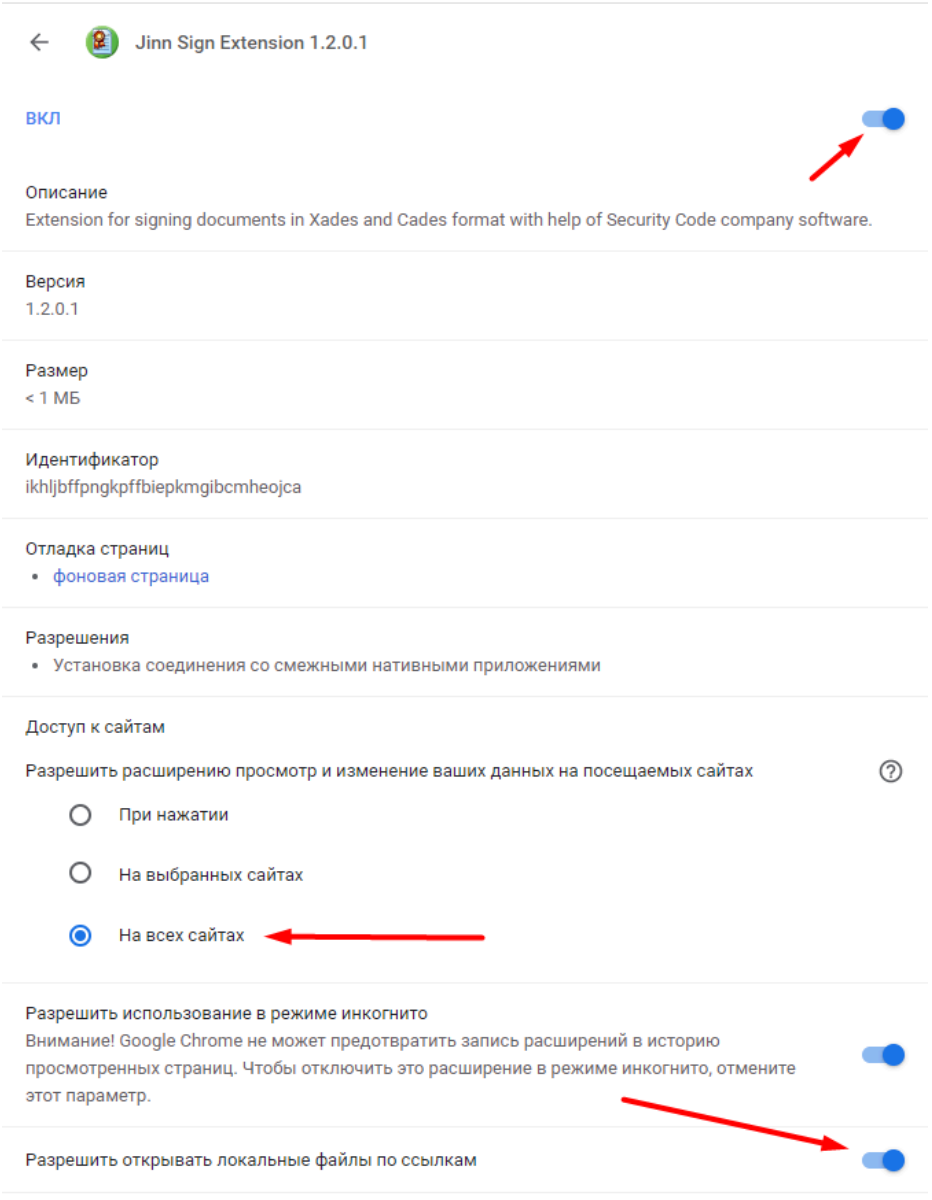


Рисунок 4.63. Выбор расширения «Jinn Sign Extension»

105) Настроить расширение в соответствии с рисунком:



106) Установка расширения Jinn Sign Extension для браузера Google Chrome на этом завершена.

107) Выполните проверку корректности установки на АРМ компонент Jinn client для работы в браузере.

4.11.2.2 Mozilla Firefox

Для установки расширения Jinn Sign Extension 1.0.0.2 в браузере Mozilla Firefox необходимо:

1) Скачать через любой браузер из сети Интернет файл с расширением по ссылке https://is.gd/8p3Ckq

108) Открыть браузер Mozilla Firefox, перейти в раздел «Дополнения > Расширения». В появившемся окне щёлкнуть по значку в верхней части экрана  , выбрать пункт «Установить дополнение из файла…».

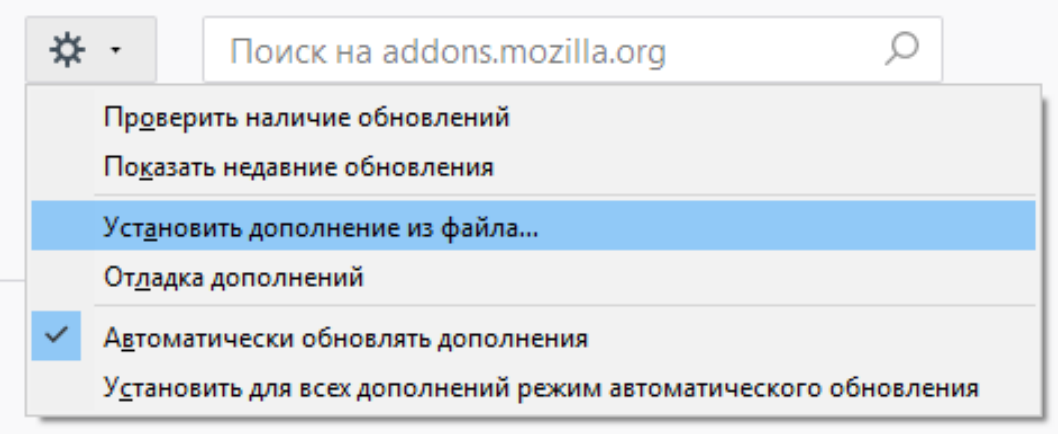


Рисунок 4.64. Окно выбора установки дополнения из файла

109) Выбрать скачанный файл из п.1. Появится контекстное окно с предложением добавить разрешения для Jinn Sign Extension.

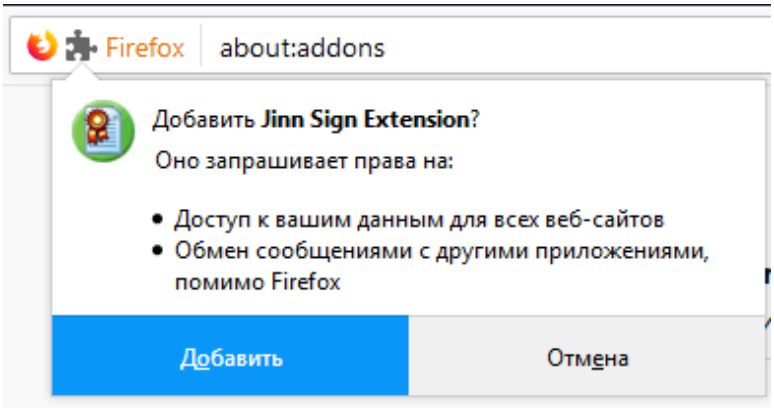


Рисунок 4.65. Окно с подтверждением установки расширения Jinn Sign Extension

110) Нажать кнопку «Добавить». Об успешной установке расширения Jinn Sign Extension будет свидетельствовать появившееся окно с соответствующим сообщением.

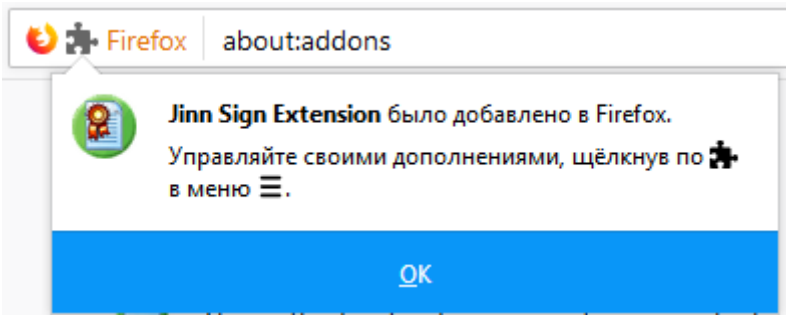


Рисунок 4.66. Сообщение об успешном завершении установки расширения Jinn Sign Extension

111) Нажать кнопку «ОК».

112) Установка расширения Jinn Sign Extension для браузера Mozilla Firefox на этом завершена.

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

114) Выполните проверку корректности установки на АРМ компонент Jinn client для работы в браузере.

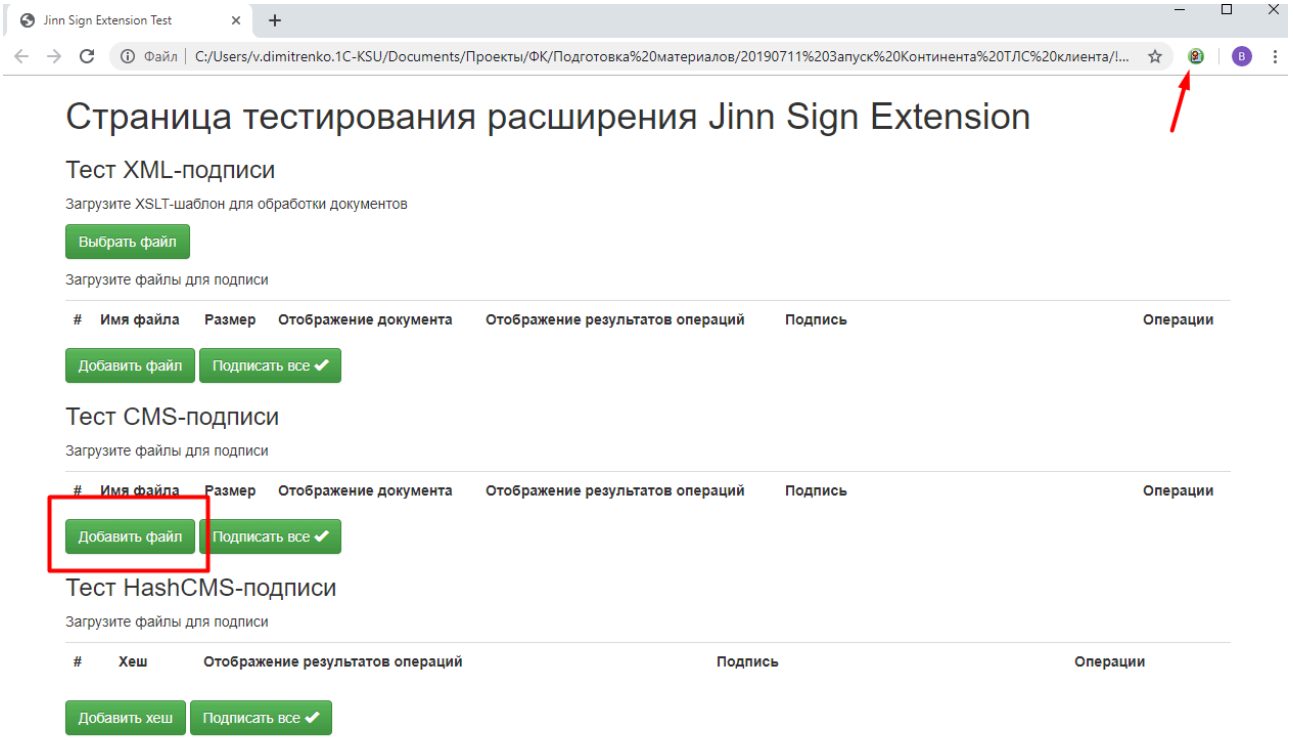
4.11.3 Проверка корректность установки компонент Jinn-Client на АРМ

Для проверки корректности установки на АРМ компонент Jinn client для работы в браузере необходимо:

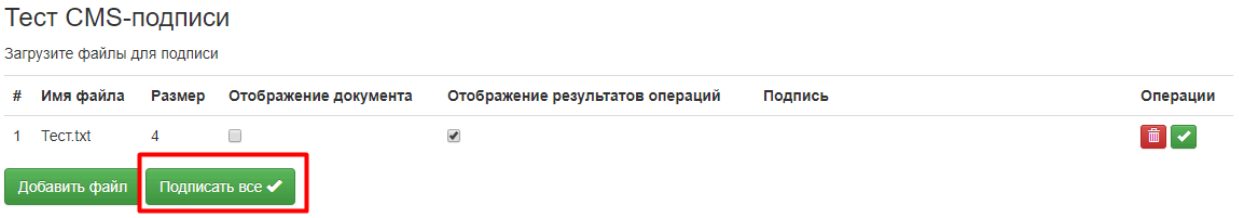
1) Откройте тестовую страницу для проверки корректности установки компонент Jinn Client.

Проверка работы подписания.7z

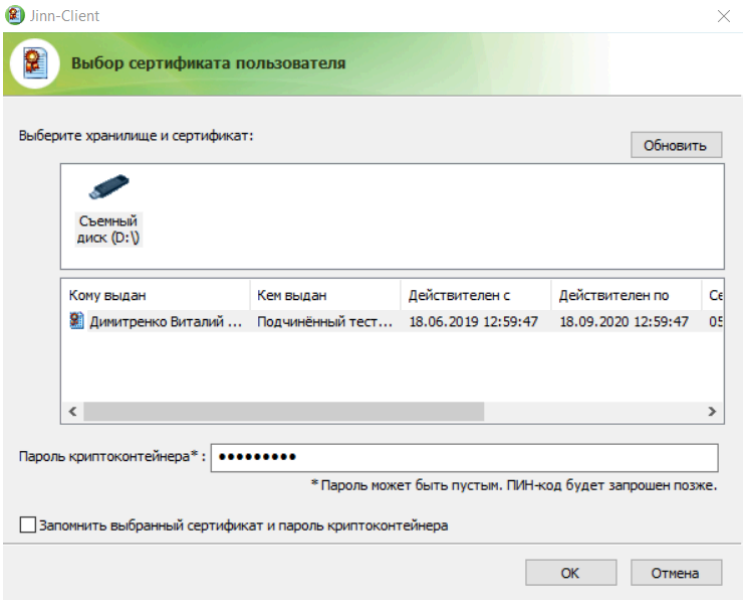
2) Расширение Jinn Sign Extension должно быть включено. Нажмите «Добавить файл» в разделе «Тест CMS-подписи» и выберете произвольный файл для тестирования (например: текстовый).



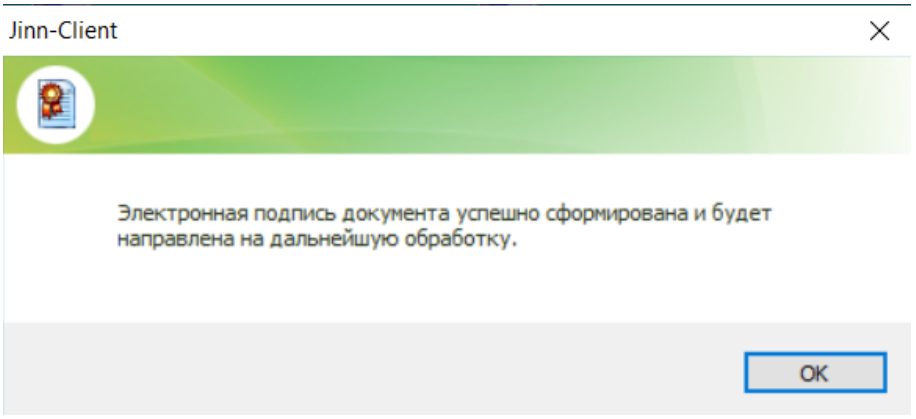
3) После загрузки файла нажмите «Подписать все»



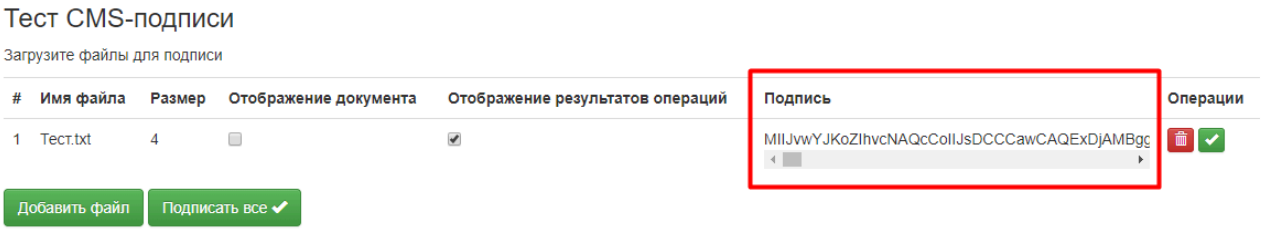
4) В открывшемся окне Jinn-Client выберите хранилище и сертификат



5) В случае успеха выведется информационное окно:

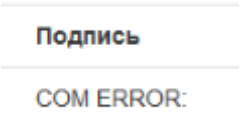


6) Нажмите «Ок». На тестовой странице в блоке подпись будет выведена подпись документа.



7) В случае проблем с установкой компонент Jinn-Client на АРМ в разделе «Подпись» будет выведена ошибка:

   a. Для ошибки «COM ERROR» рекомендуется переустановить Jinn Sign Extension Provider



4.12 Настройка Подсистемы при работе через браузер

4.12.1 Google Chrome

4.12.1.1 Установка расширения для АРМ в Интернет

Установка расширения для работы с 1С:Предприятием для браузера Google Chrome осуществляется через интернет-магазин Chrome (доступен по ссылке из сети Интернет https://chrome.google.com/webstore/category/extensions) .

Необходимо:

1) Открыть магазин Google Chrome.

115) Выполнить поиск по ключевым словам «1С:Предприятие». Среди результатов поиска выбрать «Расширение для работы с 1С:Предприятием».

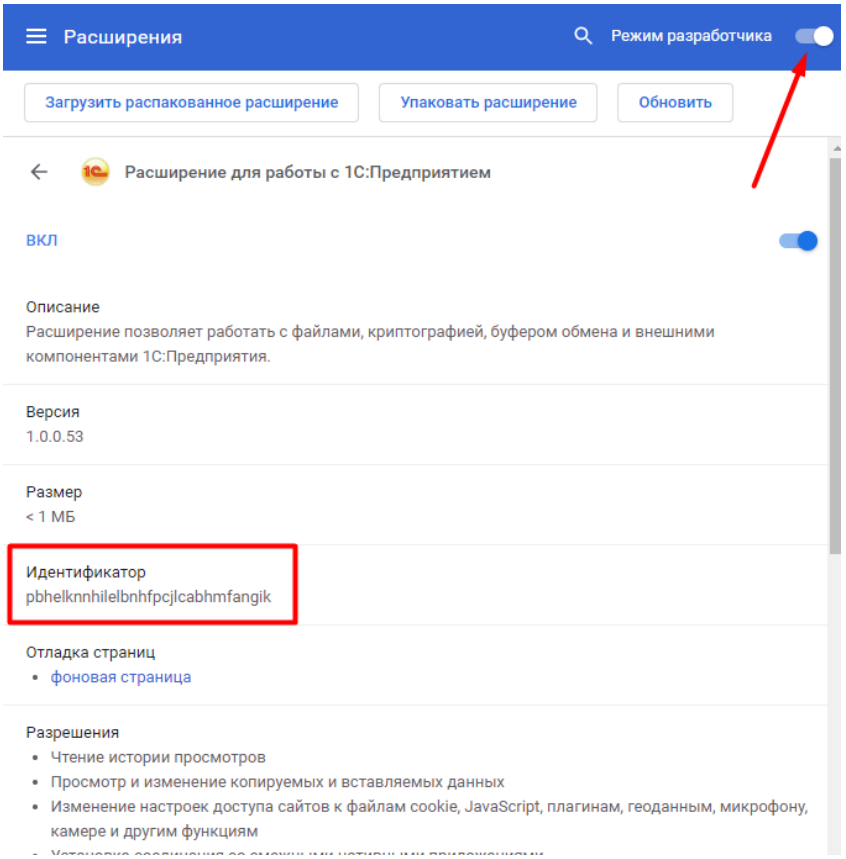
116) Установить расширение.

117) Перезагрузить браузер.

4.12.1.2 Установка расширения для АРМ в ЗКВС

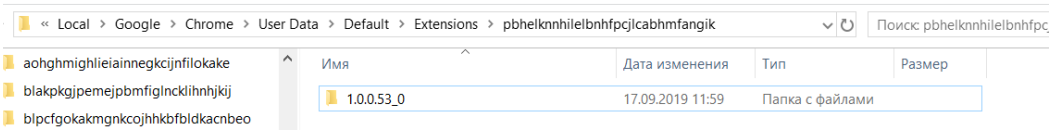
Предварительно необходимо на АРМ в Интернете сформировать распакованный пакет с расширением для работы с 1С:Предприятием.

1) На АРМ в Интернете откройте раздел Chrome с расширениями chrome://extensions/, выберете расширение для работы с 1С:Предприятием и включите режим разработчика.



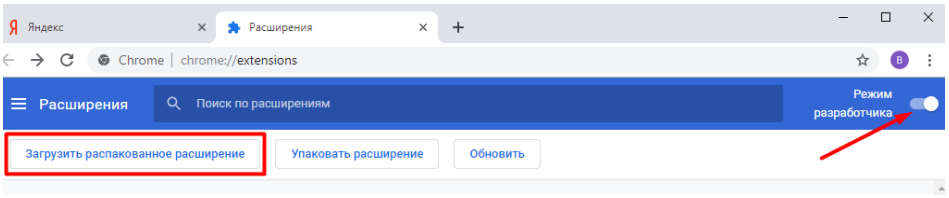
118) Откройте папку в Проводнике C:\Users\%Имя пользователя%\AppData\Local\Google\Chrome\User Data\Default\Extensions\%Идентификатор расширения%\

119) Сохраните папку 1.0.0.53_0 на флешку для переноса на АРМ в ЗКВС

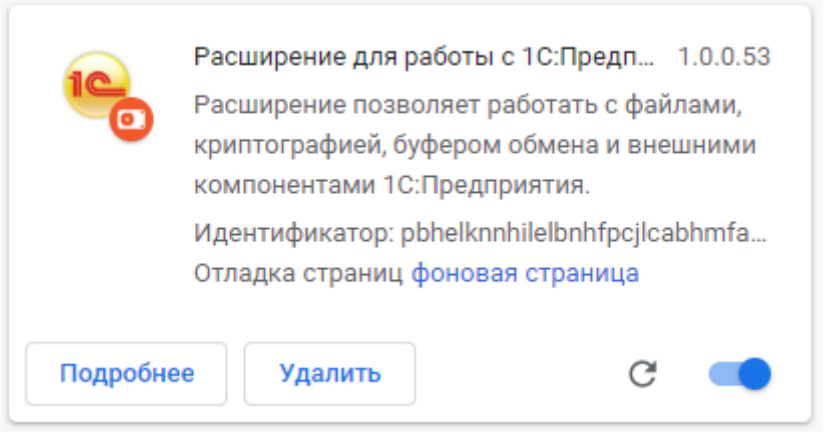


120) Перенесите данную папку на АРМ в ЗКВС.

121) Откройте на АРМ в ЗКВС раздел Chrome с расширениями chrome://extensions/, включите режим разработчика и нажмите «Загрузить распакованное расширение»:



122) В разделе расширения появится установленное расширение:



123) Отключите режим разработчика.

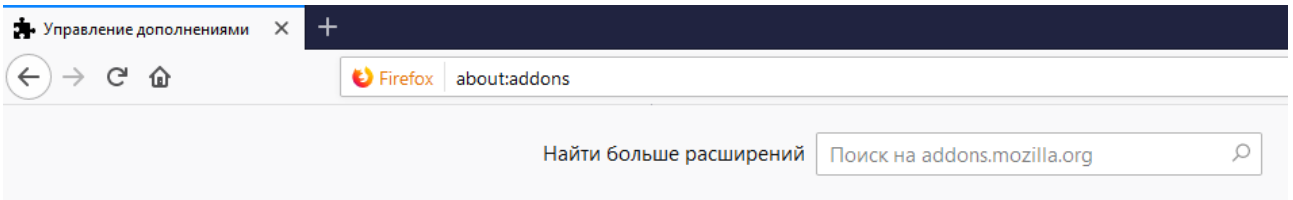
124) Перезагрузить браузер.

4.12.2 Mozilla Firefox

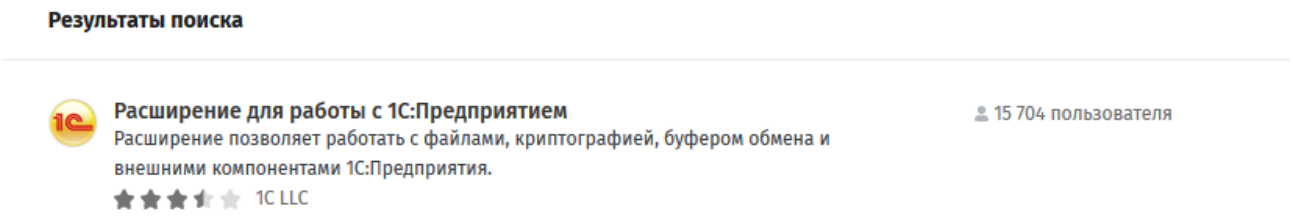
4.12.2.1 Установка дополнения для АРМ в Интернет

Для установки дополнения для работы с 1С:Предприятием для браузера Mozilla Firefox необходимо:

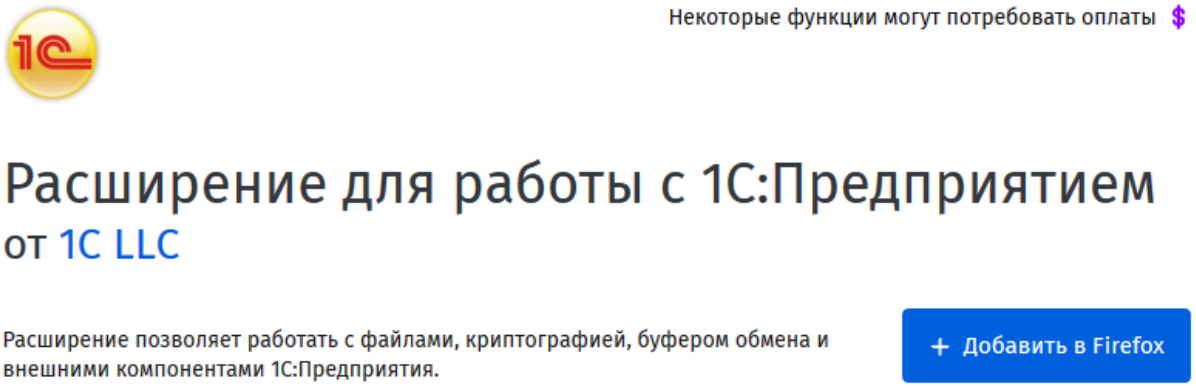
1) запустить в браузере страницу Управления дополнениями about:addons.



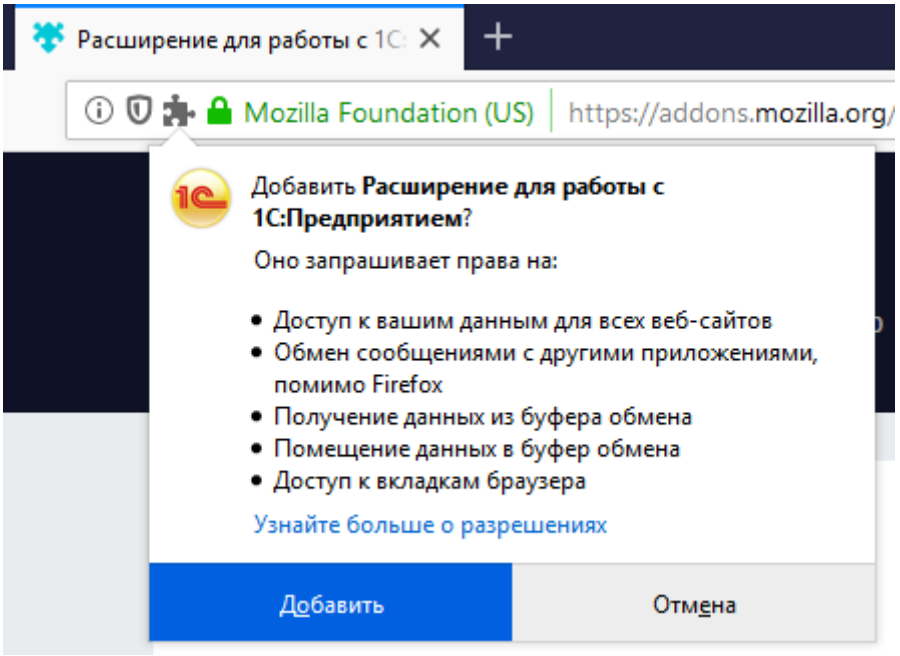
125) выполнить поиск по ключевым словам «1С:Предприятие». Среди результатов поиска выбрать «Расширение для работы с 1С:Предприятием».



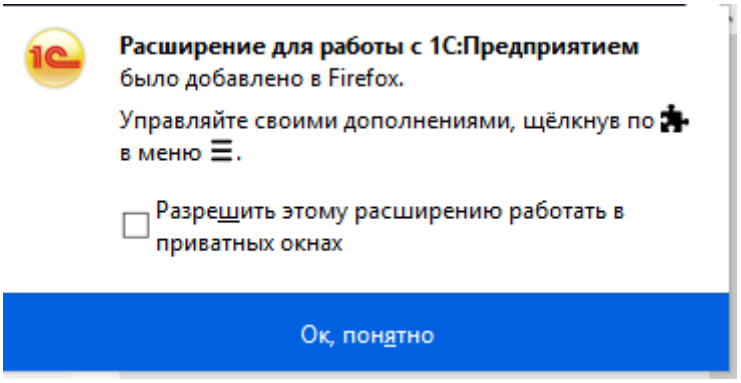
126) Установить расширение нажав «Добавить в Firefox».



127) В открывшемся окне подтвердите разрешения для дополнения нажатием «Добавить»



128) Дополнение установлено. Нажать «Ок, понятно».

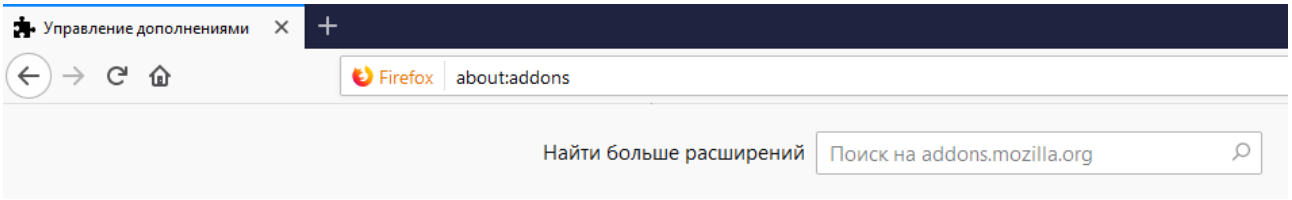


129) Перезагрузить браузер

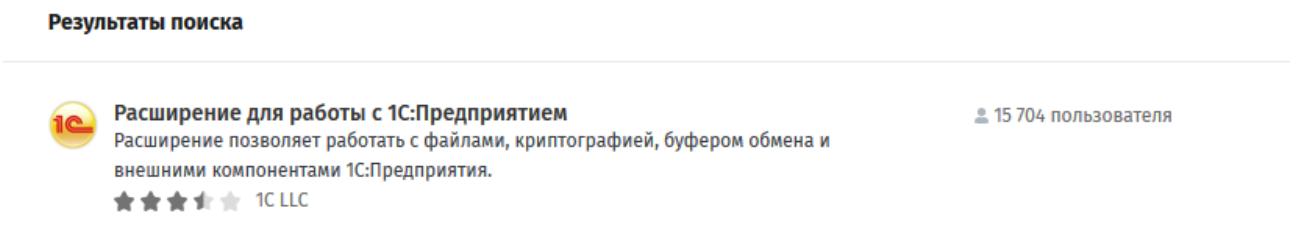
4.12.2.2 Установка дополнения для АРМ в ЗКВС

Предварительно необходимо на АРМ в Интернете сформировать пакет с расширением для работы с 1С:Предприятием. Для это необходимо:

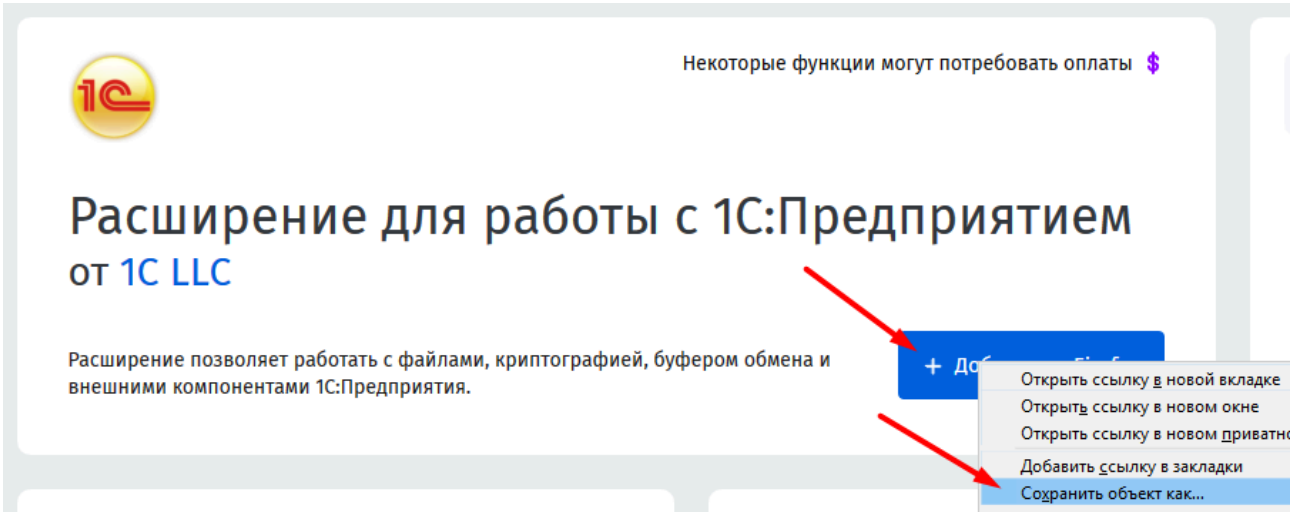
1) запустить в браузере страницу Управления дополнениями about:addons.



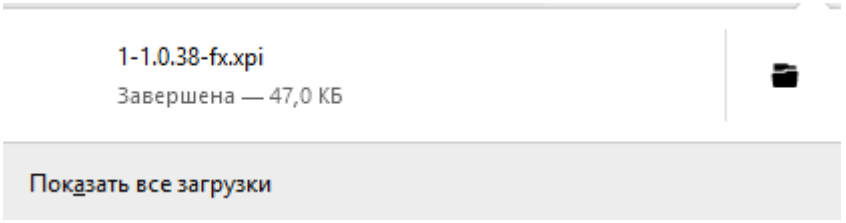
130) выполнить поиск по ключевым словам «1С:Предприятие». Среди результатов поиска выбрать «Расширение для работы с 1С:Предприятием».



131) Открыть контекстное меню нажав правой клавишей мышки на кнопке «Добавить в Firefox» и выбрать пункт «Сохранить объект как…»

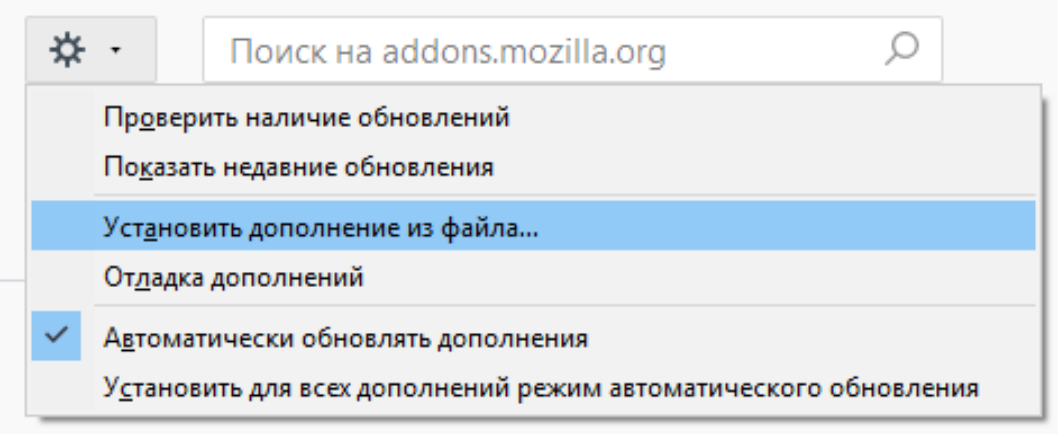


132) Выбрать папку на АРМ для сохранения пакета с расширением .xpi. Откроется информационное окно с подтверждением удачной выгрузки пакета

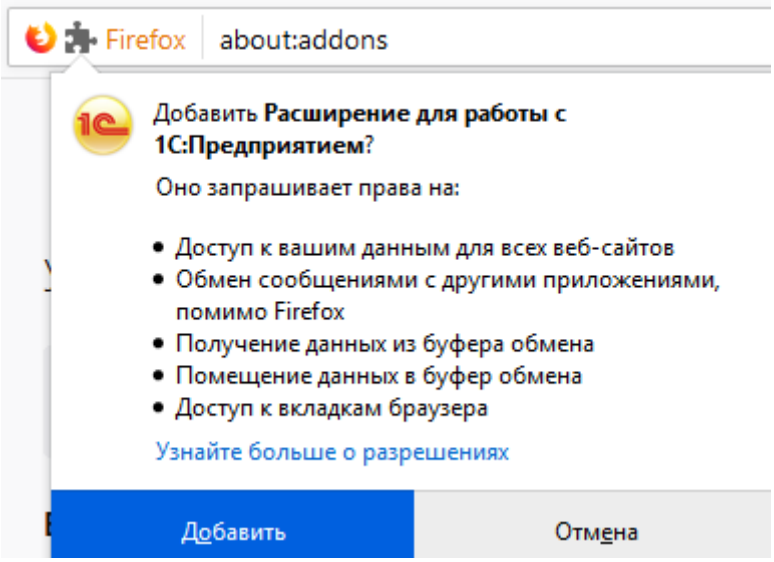


133) Перенесите данный файл на АРМ в ЗКВС

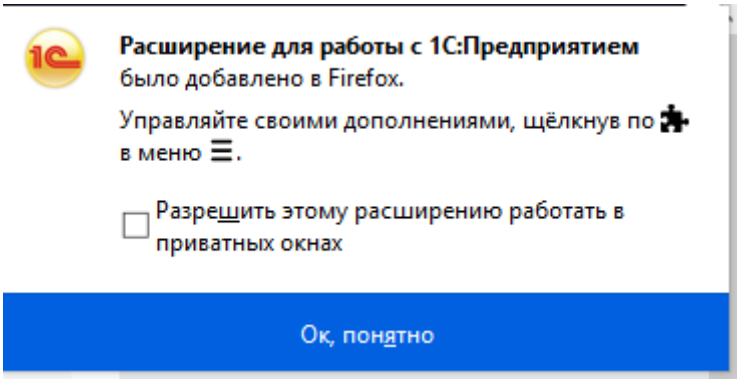
134) Открыть браузер Mozilla Firefox, перейти в раздел «Дополнения > Расширения». В появившемся окне щёлкнуть по значку в верхней части экрана  , выбрать пункт «Установить дополнение из файла…».



135) Выбрать скачанный файл, появится контекстное окно с предложением добавить разрешения расширению для работы с 1С:Предприятием.



136) Дополнение установлено. Нажать «Ок, понятно».

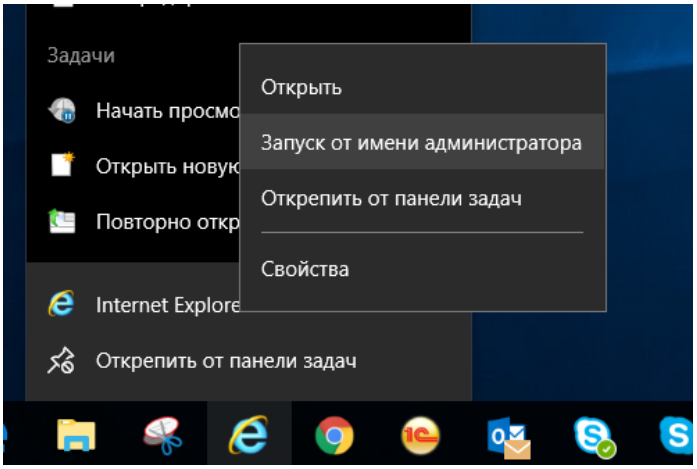


137) Перезагрузить браузер

4.12.3 Установка локальных расширений для всех браузеров

Для выполнения последующих действий пользователь должен обладать правами локального администратора.

1) Запустить веб-обозреватель от имени администратора выбрав в контекстном меню ярлыка запуска веб-обозревателя пункт «Запуск от имени администратора»



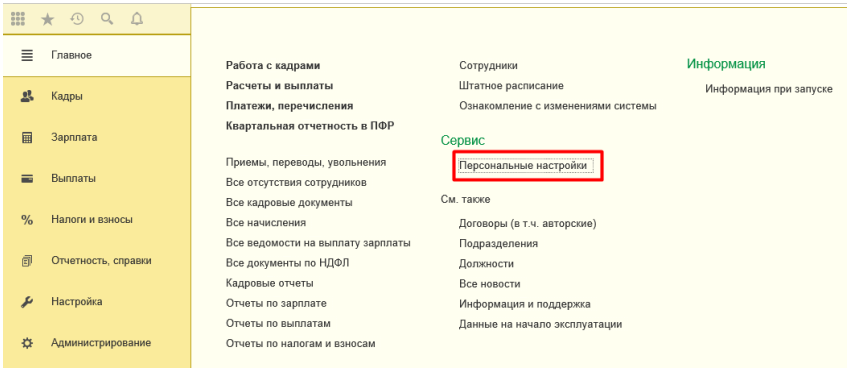
138) Зайти на стартовую страницу согласно разделу 5

139) Зайти в доступные области данных организаций.

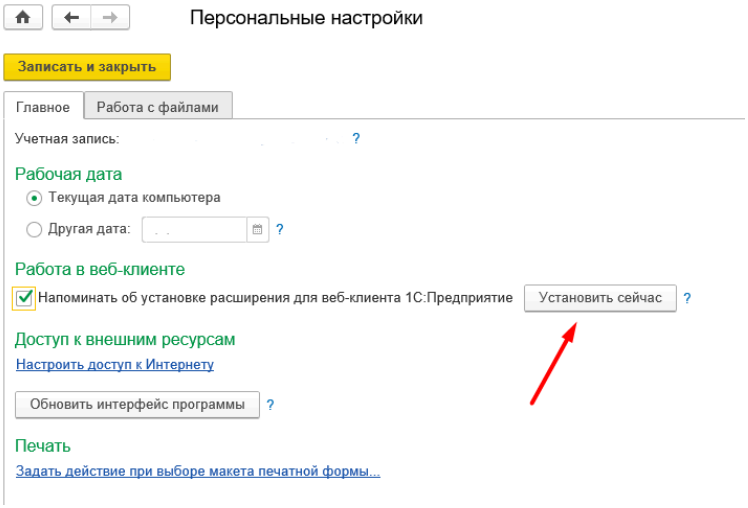
140) В зависимости от конфигурации приложения выполнить установку расширения для работы с файлами:

a) Зарплата и кадры государственного учреждения

- В разделе «Главное» выбрать подраздел «Персональные настройки»

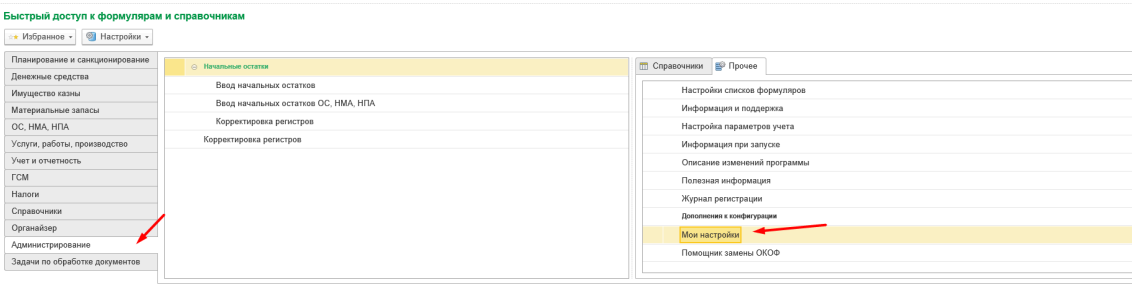


- В открывшемся окне нажать кнопку «Установить сейчас»

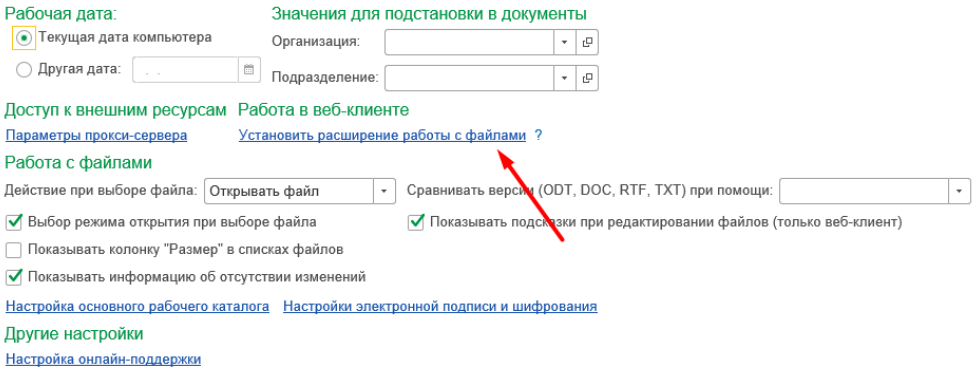


v) Бухгалтерия государственного учреждения

- В разделе «Администрирование» выбрать подраздел «Мои настройки»



- В открывшемся окне запустить «Установить расширение работы с файлами»



141) Закрыть Подсистему выбрав в меню «Файл» => «Выход»

142) Закрыть веб-обозреватель

143) Перезагрузить АРМ

4.13 Установка Тонкого клиента 1С

Для работы с 1С можно использовать Тонкий клиент 1С. Для установки тонкого клиента необходимо:

1) Запустить установочный комплект Тонкого клиента 1С в соответствии с разрядностью операционной системы и используемым релизом платформы 1С. Нажать «Далее».

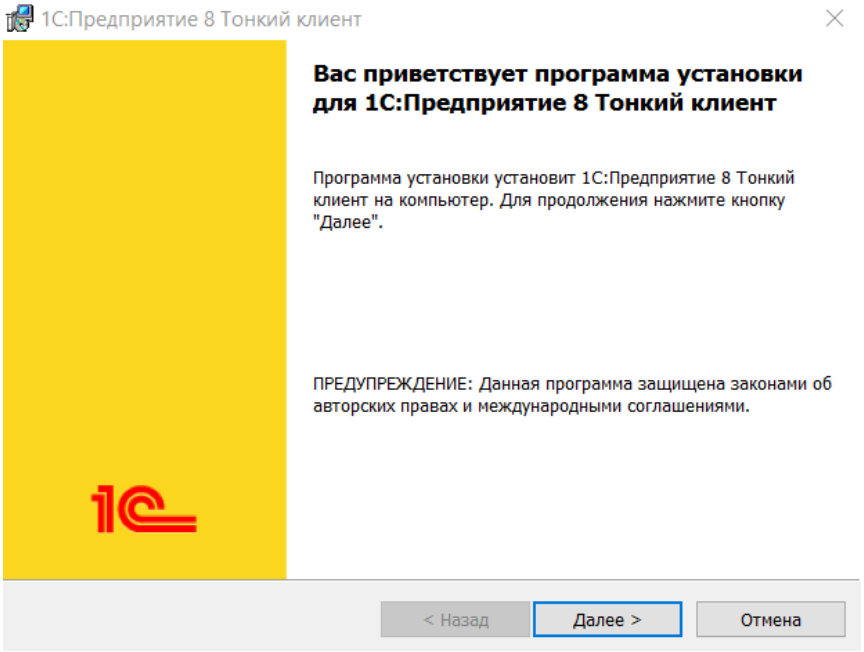


Рисунок 4.67. Программа установка Тонкого клиента 1С

144) В открывшемся окне выбрать место установки и нажать «Далее».

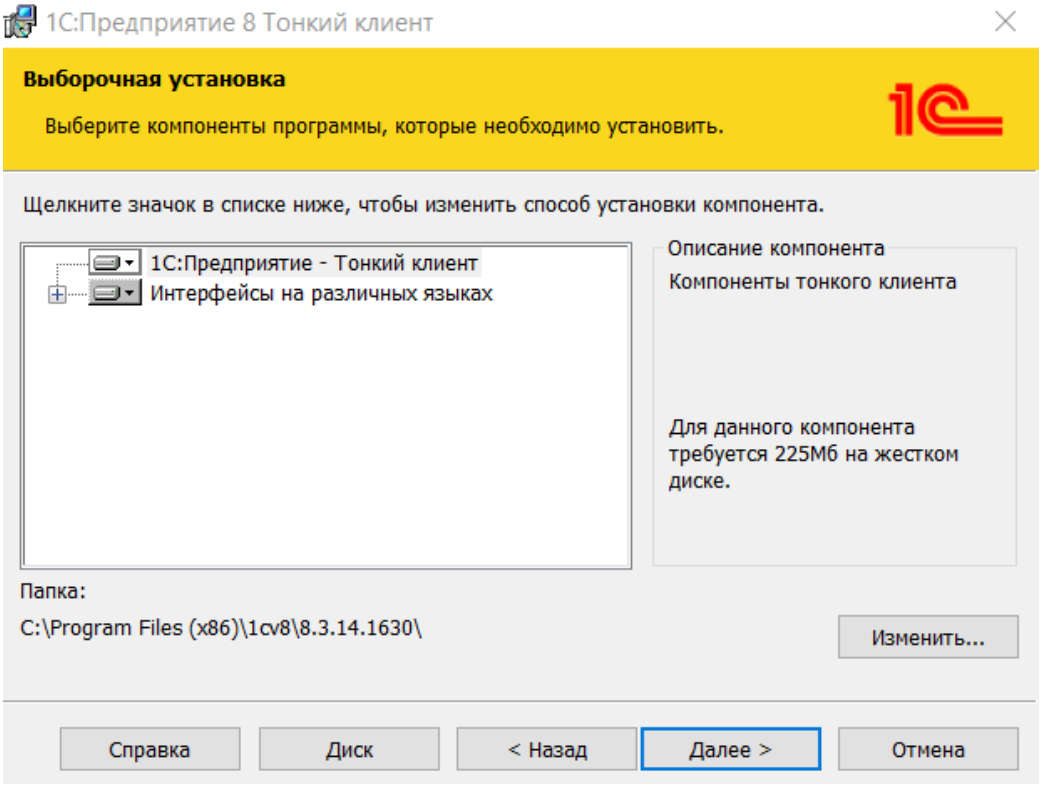


Рисунок 4.68. Выбор компонент установки Тонкого клиента 1С

145) В открывшемся окне выбрать язык «Русский» и нажать «Далее».

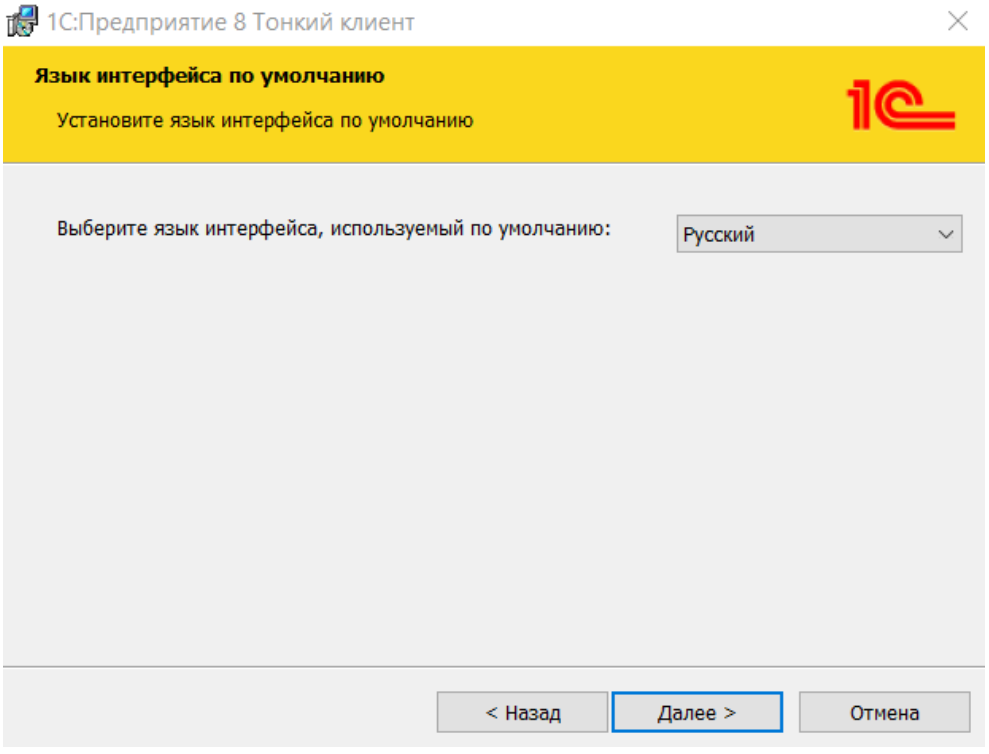


Рисунок 4.69. Выбор языка интерфейса по умолчанию

146) В открывшемся окне нажать «Установить».

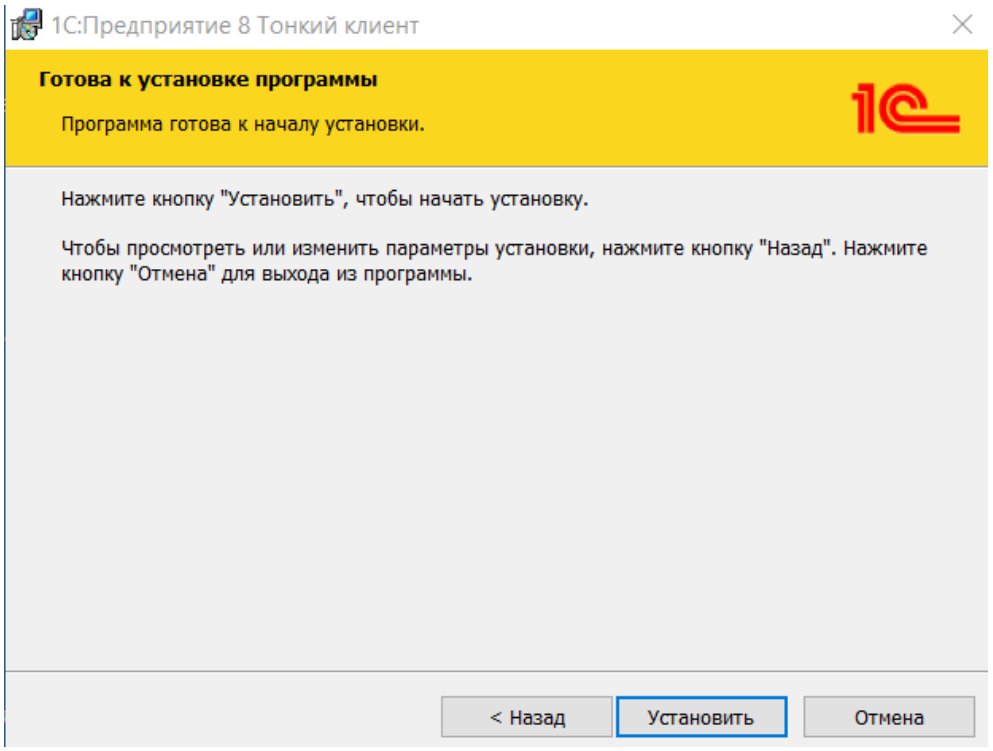


Рисунок 4.70. Установка Тонкого клиента 1С

147) В открывшемся окне нажать «Готово».

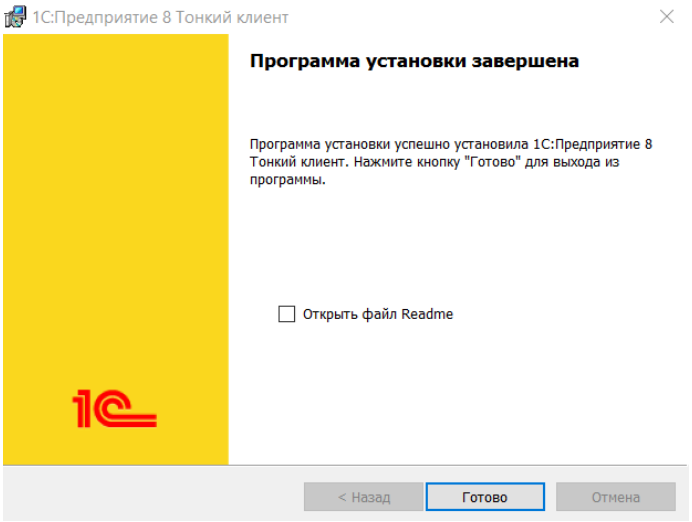


Рисунок 4.71. Завершение установка Тонкого клиента 1С

4.14 Настройка Тонкого клиента 1С

Для настройки тонкого клиента необходимо:

1) Запустите Стартовую страницу http://buh2012.budget.gov.ru/buh2012/

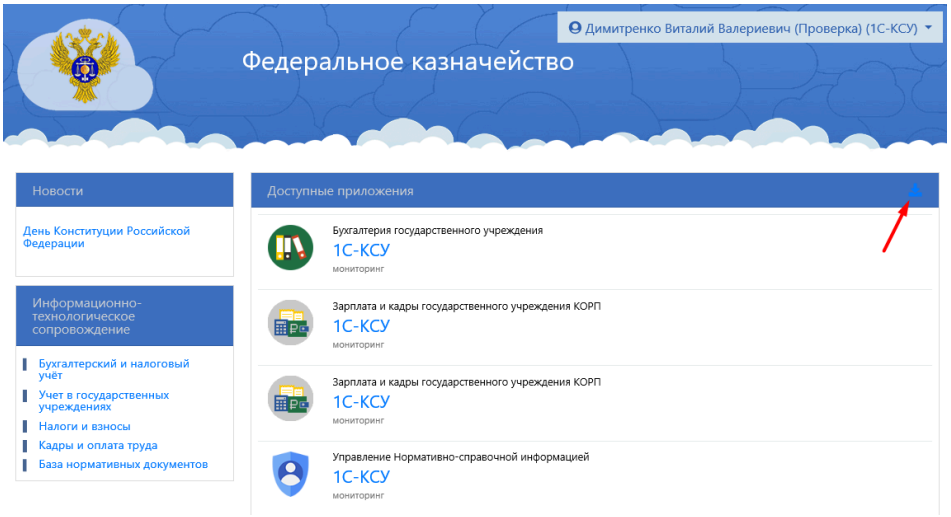


Рисунок 4.72. Стартовая страница

На Стартовой странице выберете пункт меню для скачивания настроечного файла.

148) В открывшемся сообщении выберите «Сохранить как».

Рисунок 4.73. Сохранение настроечного файла

149) В качестве места сохранения укажите Рабочий стол. Укажите название файла «ПУНФА&ПУОТ.v8i» и нажмите «Сохранить».

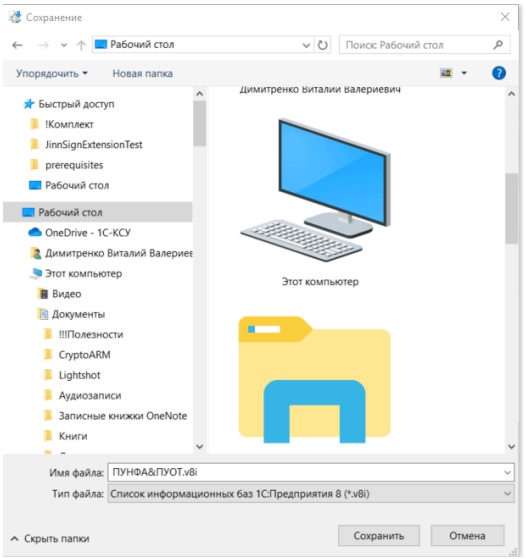
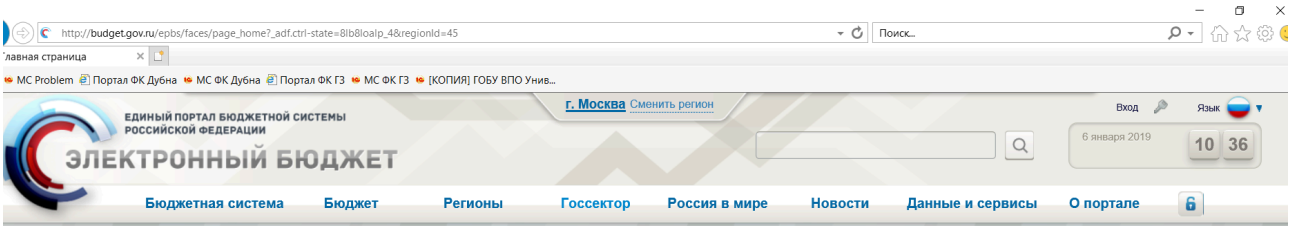


Рисунок 4.74. Сохранение файла ПУНФА&ПУОТ.v8i на рабочий стол

5 Процедура входа пользователя в Подсистему

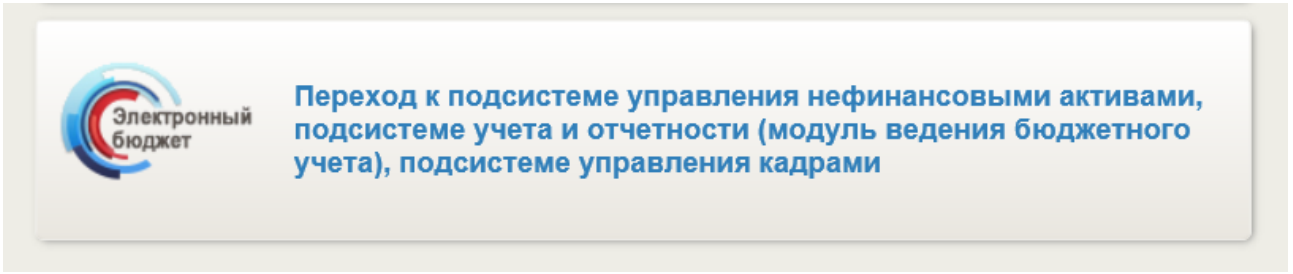
5.1 Процедура входа при работе через браузер

1) Открыть в веб-обозревателе адрес http://budget.gov.ru



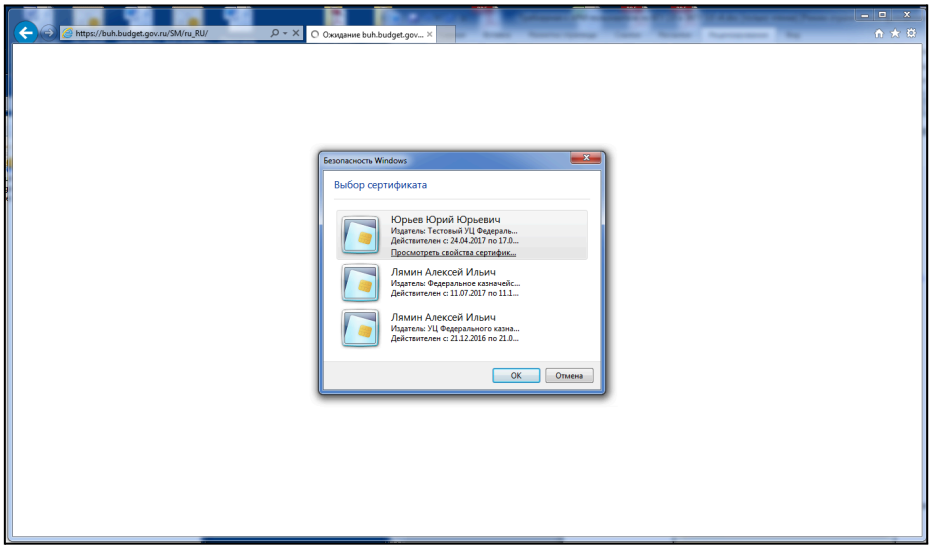
150) На открывшейся странице Единого портала бюджетной системы Российской федерации выбрать ссылку «Вход»

151) На открывшейся странице в разделе «Закрытая часть единого портала бюджетной системы Российской Федерации» выбрать подраздел для перехода к подсистеме управления нефинансовыми активами, подсистеме учета и отчетности (модуль ведения бюджетного учета), подсистеме управления кадрами

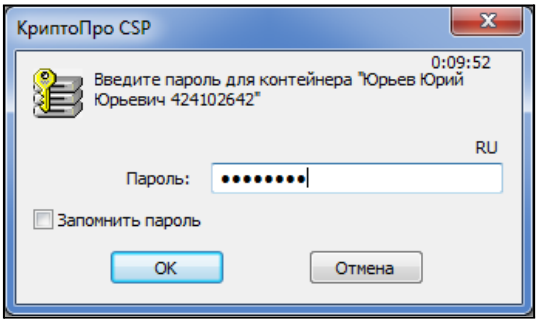


152) На экране отобразится меню выбора сертификата пользователя

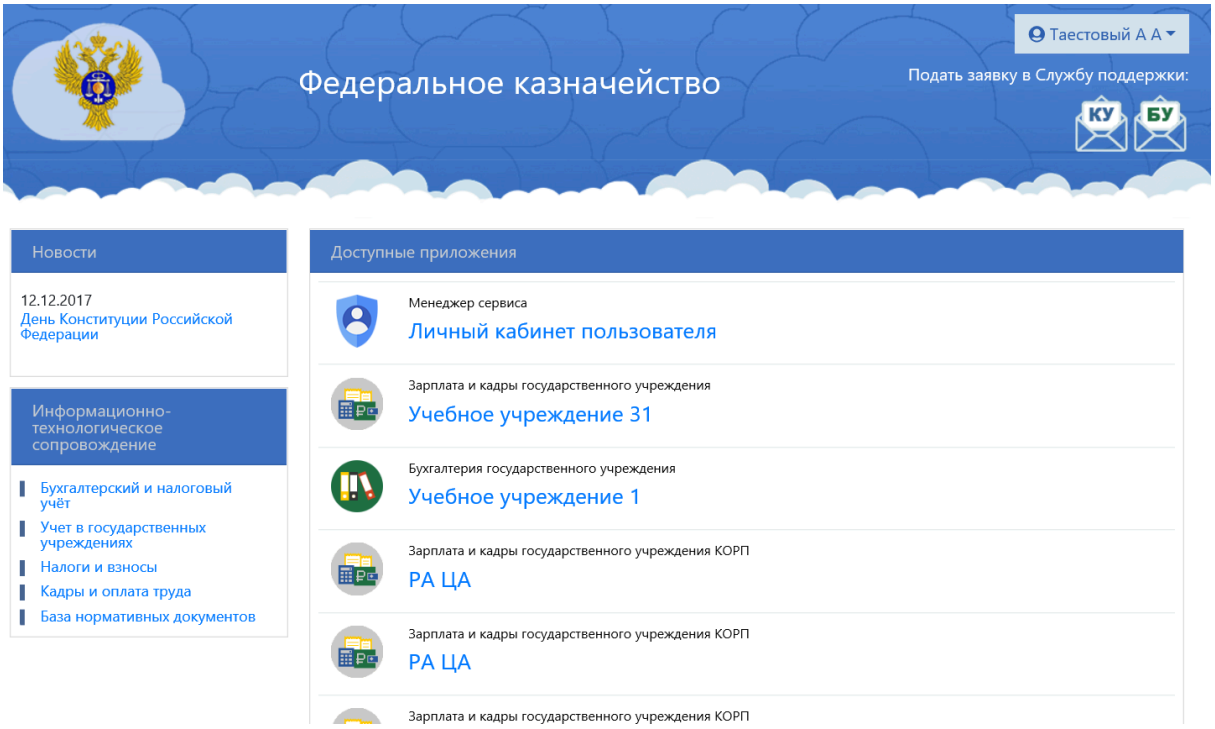
153) Выбрать сертификат пользователя для обеспечения создания безопасного соединения.



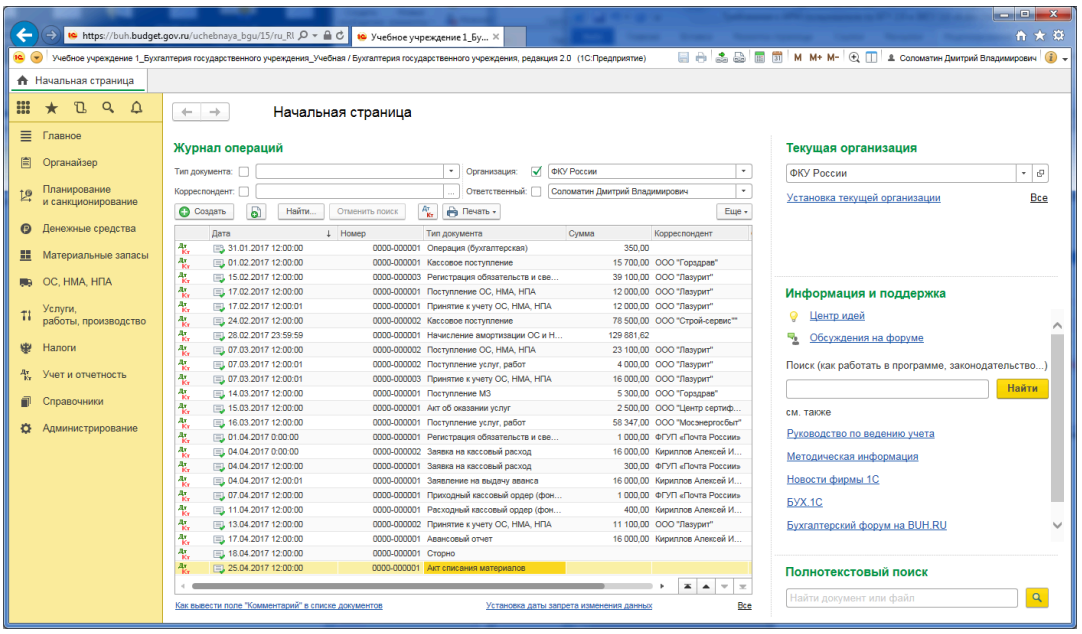
154) Ввести пароль для контейнера



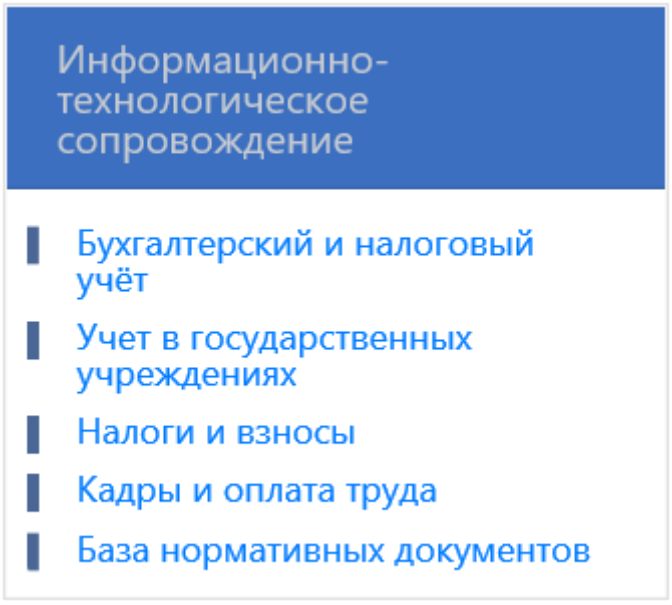
155) Отобразится форма «Стартовой страницы пользователя» с перечнем областей данных, доступных пользователю.



156) Выбрать из раздела «Доступных приложений» необходимое приложение. Отобразится соответсветствующая область данных



157) Для доступа к ресурсу «Информационно-технологического сопровождения» необходимо выбрать соответствующую ссылку в разделе «Информационно-технологическое сопровождение» Стартовой страницы.



5.2 Процедура входа при работе через Тонкий клиент 1С

Перед запуском Тонкого клиента необходимо запустить Континент ТЛС клиент. Для того, чтобы убедиться в том, что Континент ТЛС клиент включен и настроен можно запустить стартовую страницу приложения в Google Chrome

http://buh2012.budget.gov.ru/buh2012/

Для запуска Тонкого клиента 1С необходимо:

1) Запустить с рабочего стола файл «ПУНФА&ПУОТ.v8i», выберите необходимую область данных и нажмите «1С:Предприятие».

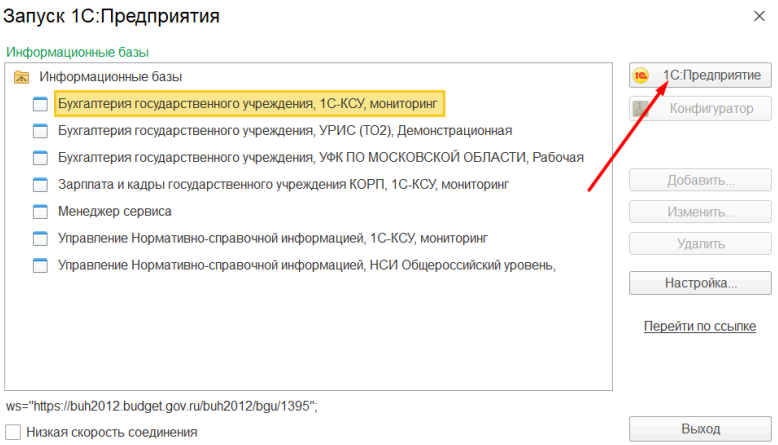


Рисунок 5.1. Запуск необходимого приложения

158) В открывшемся окне нажать «Ок».

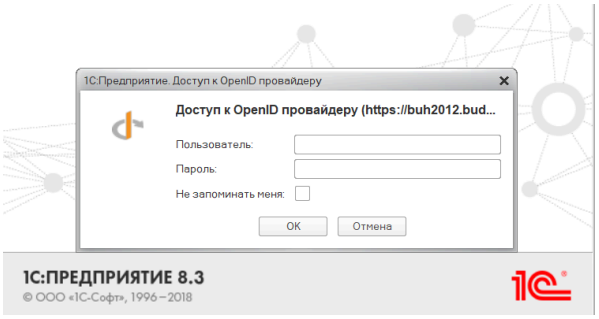


Рисунок 5.2. Доступ к OpenID

159) Приложение запущено.

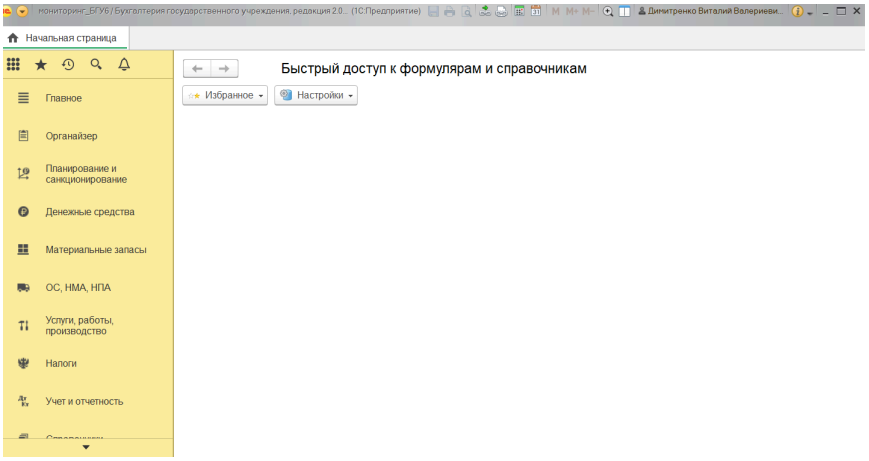


Рисунок 5.3. Приложение запущено