

**ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ
К ПОДСИСТЕМЕ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ
ГОСУДАРСТВЕННОЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ
СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ
«ЭЛЕКТРОННЫЙ БЮДЖЕТ» С ИСПОЛЬЗОВАНИЕМ
КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ**

МОСКВА

2015

АННОТАЦИЯ

Настоящий документ является инструкцией по защищенному удаленному подключению пользователей к подсистеме бюджетного планирования государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет» (далее – Система) с использованием квалифицированной электронной подписи.

СОДЕРЖАНИЕ

1. ТРЕБОВАНИЯ К АППАРАТНО-ТЕХНИЧЕСКИМ И ПРОГРАММНЫМ СРЕДСТВАМ	4
1.1. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ	4
1.2. ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	4
1.3. НАСТРОЙКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	4
1.3.1. Установка криптопровайдера «КриптоПро CSP»	4
1.3.2. Установка драйвера используемого носителя ключевой информации сертификата пользователя	6
1.3.3. Установка личного сертификата и сертификата доверенного корневого центра сертификации	12
1.3.4. Настройка Internet Explorer	21
2. ВХОД ПОДСИСТЕМУ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ «ЭЛЕКТРОННЫЙ БЮДЖЕТ»	24
3. ПРОБЛЕМЫ ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ И ИХ УСТРАНЕНИЕ.....	27
3.1. ПРОБЛЕМА С СЕРТИФИКАТОМ БЕЗОПАСНОСТИ	27
3.2. ВСТАВЬТЕ КЛЮЧЕВОЙ НОСИТЕЛЬ.....	27
3.3. НЕ УДАЕТСЯ ОТОБРАЗИТЬ ЭТУ СТРАНИЦУ	28
3.4. 403 ACCESS DENIED.....	29
3.5. НЕ УДАЕТСЯ ОТОБРАЗИТЬ ЭТУ СТРАНИЦУ. ВКЛЮЧИТЕ ПРОТОКОЛЫ TLS	29
3.6. ИНЫЕ ОШИБКИ.....	31

1. ТРЕБОВАНИЯ К АППАРАТНО-ТЕХНИЧЕСКИМ И ПРОГРАММНЫМ СРЕДСТВАМ

1.1. Требования к техническому обеспечению

Для автоматизированных рабочих мест пользователей Системы устанавливаются следующие минимальные технические требования:

- 1) Процессор с тактовой частотой не менее 600 МГц;
- 2) Объем оперативной памяти не менее 128 Мб;
- 3) Объем жесткого диска не менее 10 Гб;
- 4) Клавиатура;
- 5) Монитор SVGA (графический режим должен иметь разрешение не менее 1024x768);
- 6) USB-порт;
- 7) Квалифицированный сертификат ключа проверки электронной подписи (может быть предоставлен на носителях ruToken CSP, eToken CSP);
- 8) Манипулятор типа мышь.

На рабочем месте должен быть предоставлен доступ к сети Интернет со скоростью не менее 256 Кбит/сек.

1.2. Требования к программному обеспечению

Программные средства, требуемые для обеспечения возможности подписания документов электронной подписью:

- 1) Интернет-браузер «Internet Explorer» версия 10.0 и выше;
- 2) Операционная система Windows XP и выше;
- 3) Сертифицированная версия «КриптоПро CSP» - криптопровайдер, вспомогательная программа, использующаяся для генерации электронных подписей, работы с сертификатами и т.д.

1.3. Настройка программного обеспечения

1.3.1. Установка криптопровайдера «КриптоПро CSP»

1. Загрузите и запустите установочный файл сертифицированной версии «КриптоПро CSP», доступный на странице <https://www.cryptopro.ru/products/csp/downloads>. Окно приветствия установщика «КриптоПро CSP» представлено на рисунке (Рисунок 1).

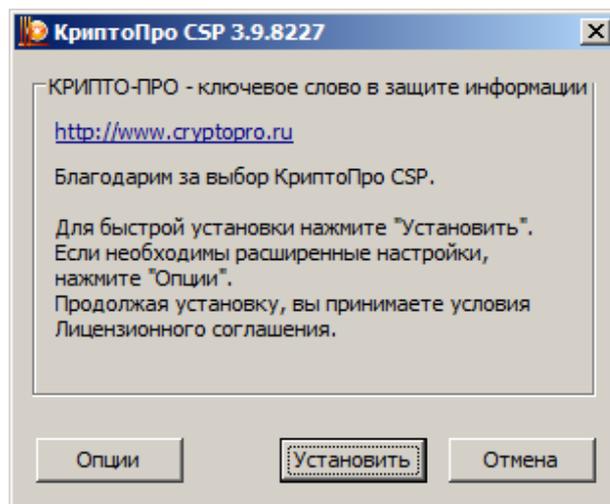


Рисунок 1. Окно приветствия «КриптоПРО CSP»

2. Нажмите кнопку «Установить». После завершения процесса установки и настройки «КриптоПРО CSP» появится сообщение об успешной установке (Рисунок 2).

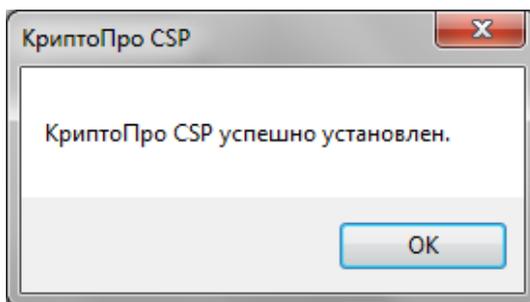


Рисунок 2. Установка «КриптоПро CSP»

При установке программы «КриптоПро CSP» может быть запрошен лицензионный ключ, который поставляется с установочным пакетом «КриптоПро CSP».

3. Запустите «КриптоПро CSP» (Пуск/Все программы/КриптоПро/КриптоПро CSP). Откройте вкладку «Настройки TLS» и приведите настройки программы в соответствии с Рисунок 3 (для перенастройки могут потребоваться права администратора на локальном компьютере и перезагрузка компьютера).

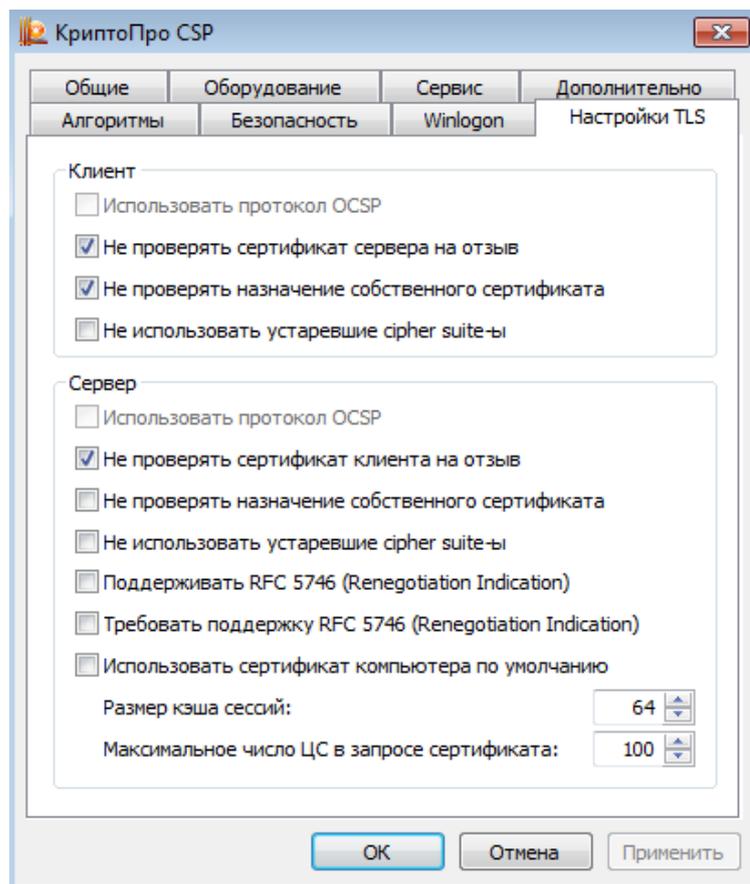


Рисунок 3. Настройки TLS

1.3.2. Установка драйвера используемого носителя ключевой информации сертификата пользователя

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

Если необходимый драйвер не установлен, необходимо:

а) Драйвер носителя типа Rutoken

1. Загрузите и запустите установочный файл, доступный на странице <http://www.rutoken.ru/support/download/drivers-for-windows/>. Окно приветствия установщика драйверов Rutoken представлено на рисунке (Рисунок 4).

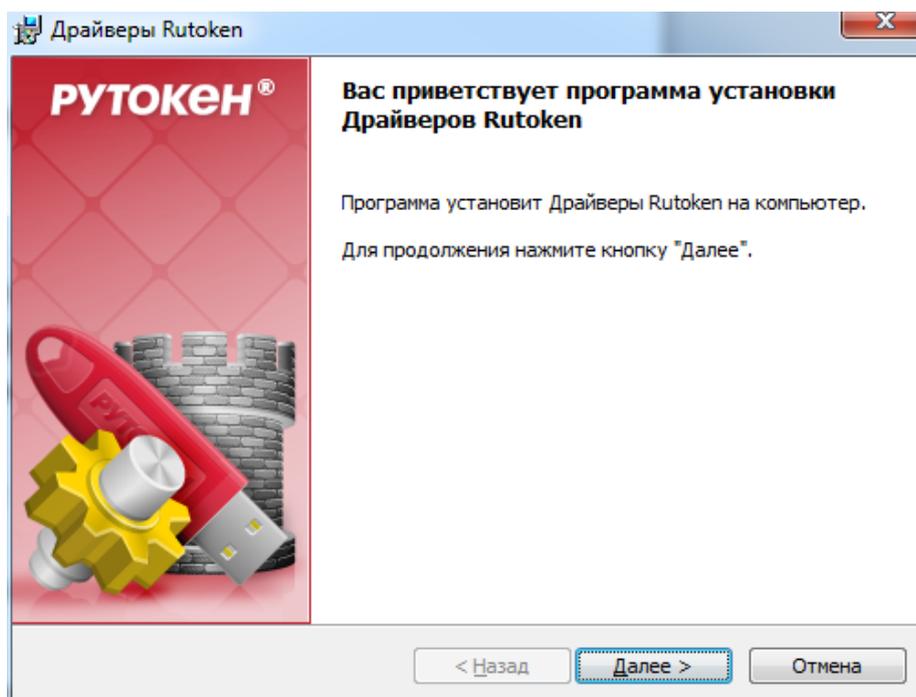


Рисунок 4. Экранная форма приветствия установщика драйвера Rutoken

2. Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов (Рисунок 5).

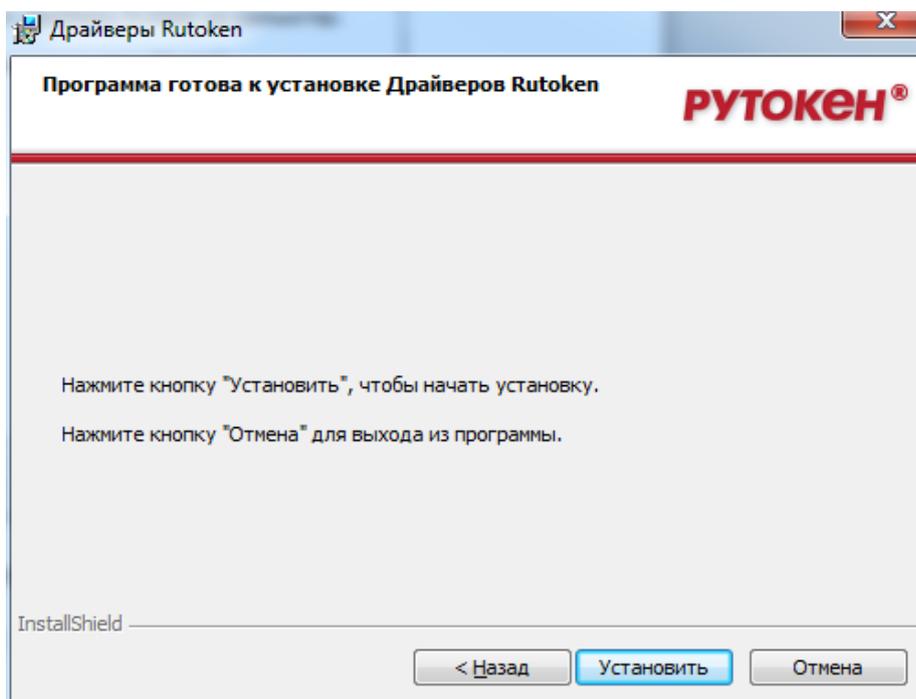


Рисунок 5. Сообщение о готовности к выполнению установки драйверов

3. Нажмите кнопку «Установить». Начнется установка драйверов Rutoken на АРМ пользователя. Установка может занять несколько минут, информация о прогрессе установки выводится в окне, представленном на рисунке (Рисунок 6).

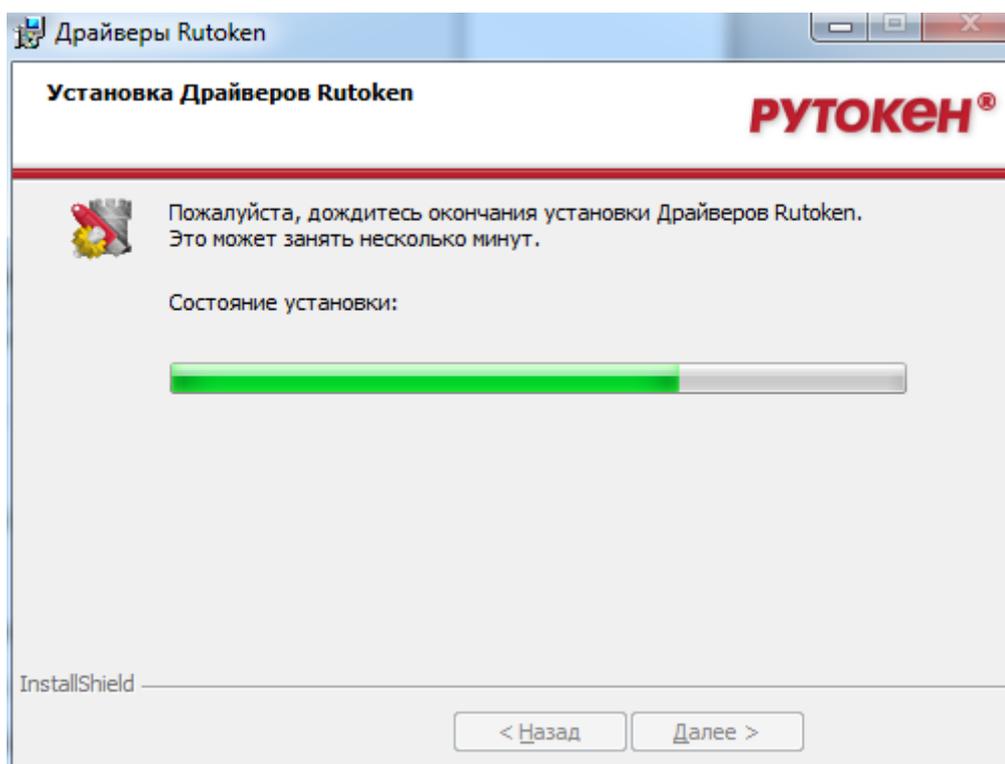


Рисунок 6. Окно, информирующее о прогрессе установки драйверов Rutoken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 7).

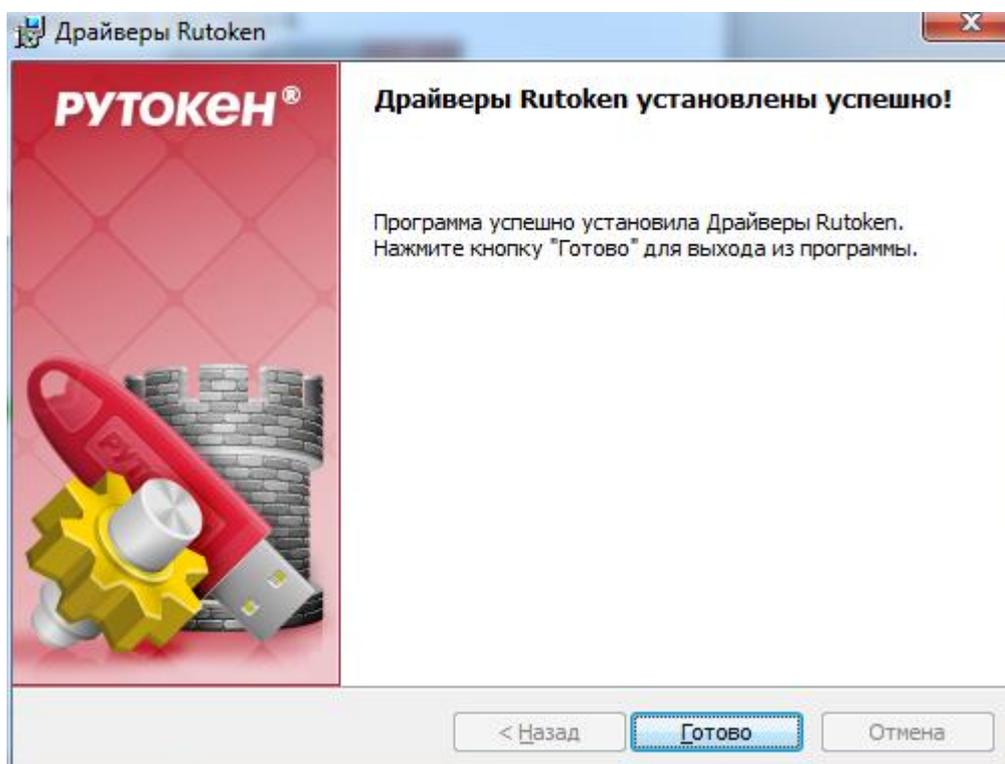


Рисунок 7. Сообщение об успешной установке драйверов Rutoken.

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

5. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места Пользователя, ответить отрицательно.

б) Драйвер носителя типа eToken

1. Загрузите и запустите установочный файл, доступный на странице <http://www.aladdin-rd.ru/support/downloads/etoken/>. Окно приветствия установщика драйвера eToken представлено на рисунке (Рисунок 8).

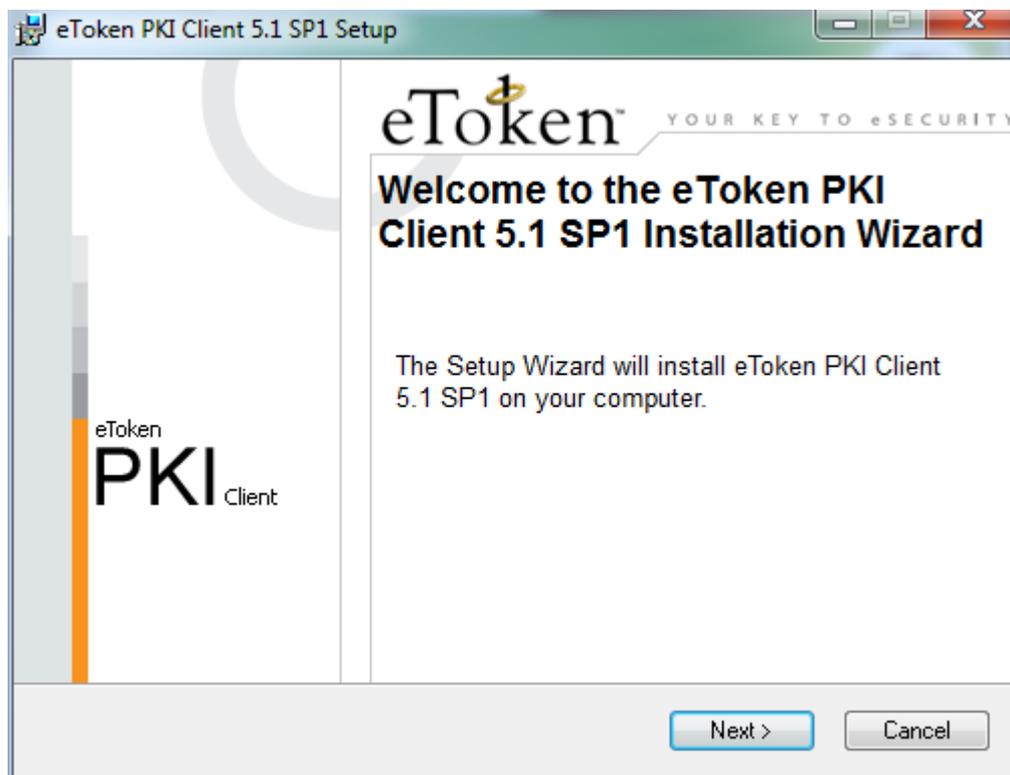


Рисунок 8. Экранная форма приветствия установщика драйверов eToken

2. Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (Рисунок 9).

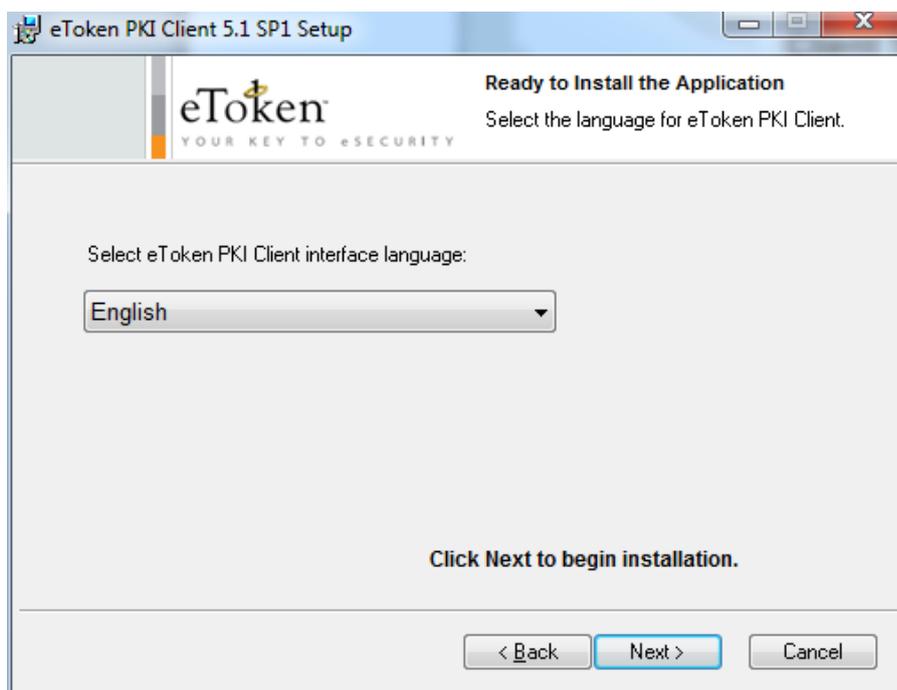


Рисунок 9. Окно выбора языка программы, управляющей ключевыми носителями eToken

3. Так как для решения задач, возникающих при работе в системе «Электронный бюджет», данное ПО не будет использоваться пользователями системы, то выбор языка можно пропустить, нажав кнопку «Next». На экране появится диалог лицензионное соглашение (Рисунок 10).

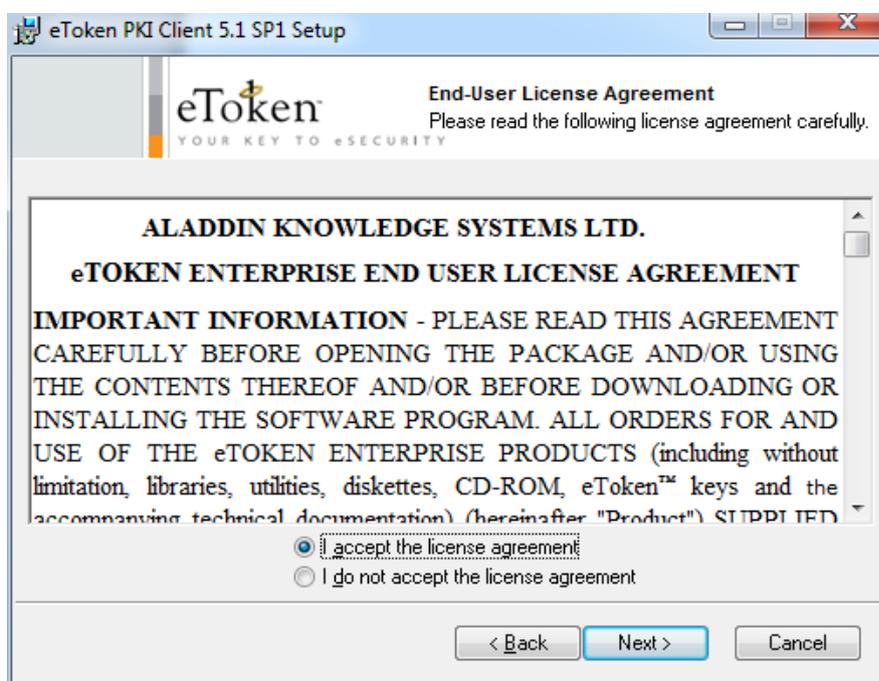


Рисунок 10. Окно просмотра лицензионного соглашения

4. Выберите пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (Рисунок 11).

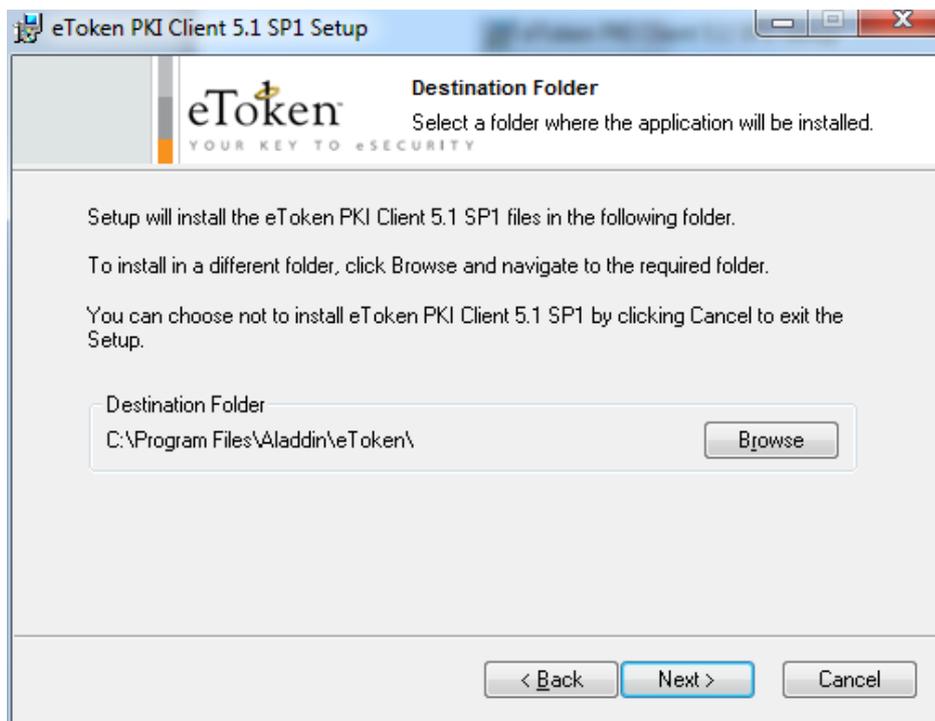


Рисунок 11. Окно выбора пути для установки программы

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

Начнется установка программы и драйверов. Диалог процесса установки представлено на рисунке (Рисунок 12).

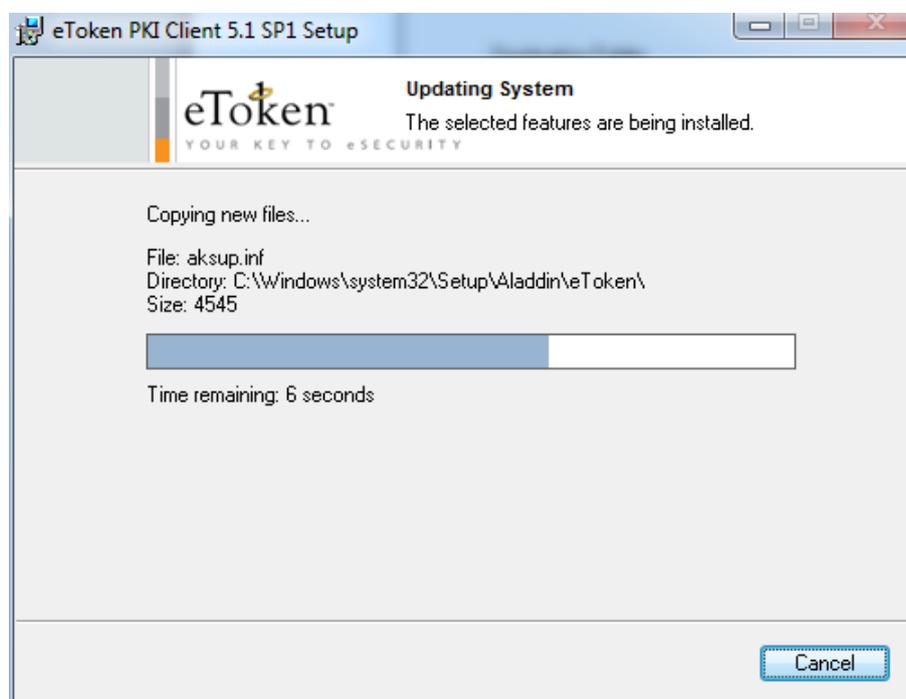


Рисунок 12. Прогресс установки драйверов eToken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 13).

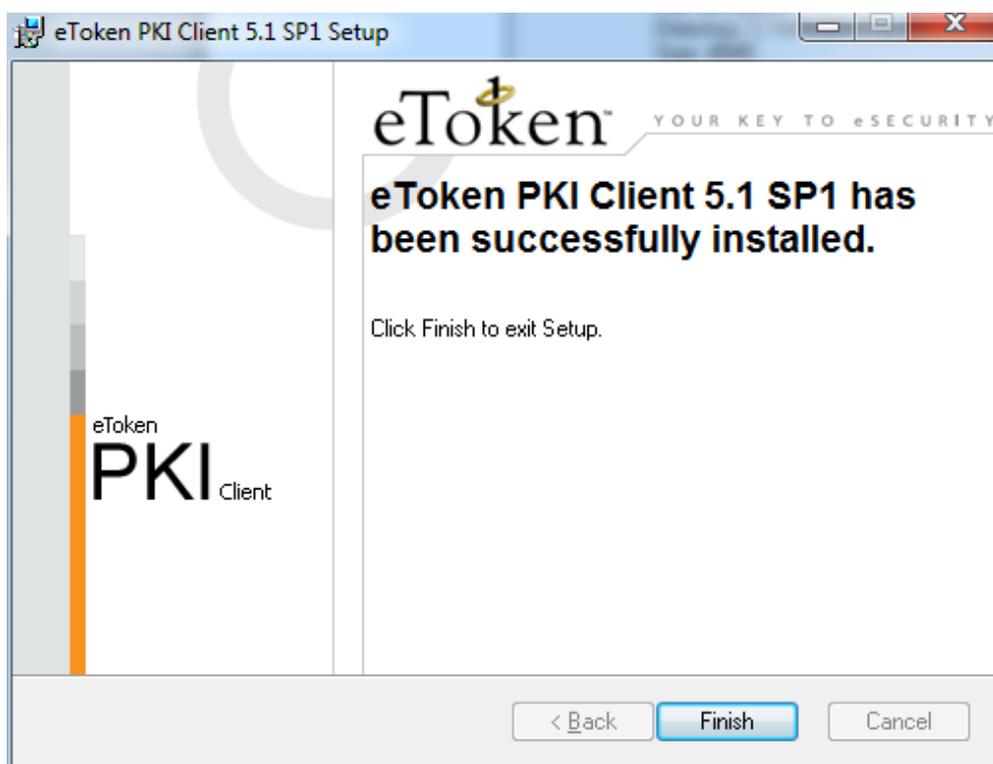


Рисунок 13. Сообщение об успешной установке драйверов Rutoken

6. Нажмите кнопку «Finish». Окно установщика драйверов будет закрыто.

7. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места пользователя, ответить отрицательно.

1.3.3. Установка личного сертификата и сертификата доверенного корневого центра сертификации

Установка сертификата пользователя и доверенного корневого центра сертификации выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в личный кабинет системы «Электронный бюджет».

Для добавления сертификатов:

1. Запустите «КриптоПро CSP» (Пуск/Все программы/КриптоПро/КриптоПро CSP). В открывшемся окне на вкладке «Сервис» необходимо нажать на кнопку «Просмотреть сертификаты в контейнере» (Рисунок 14).

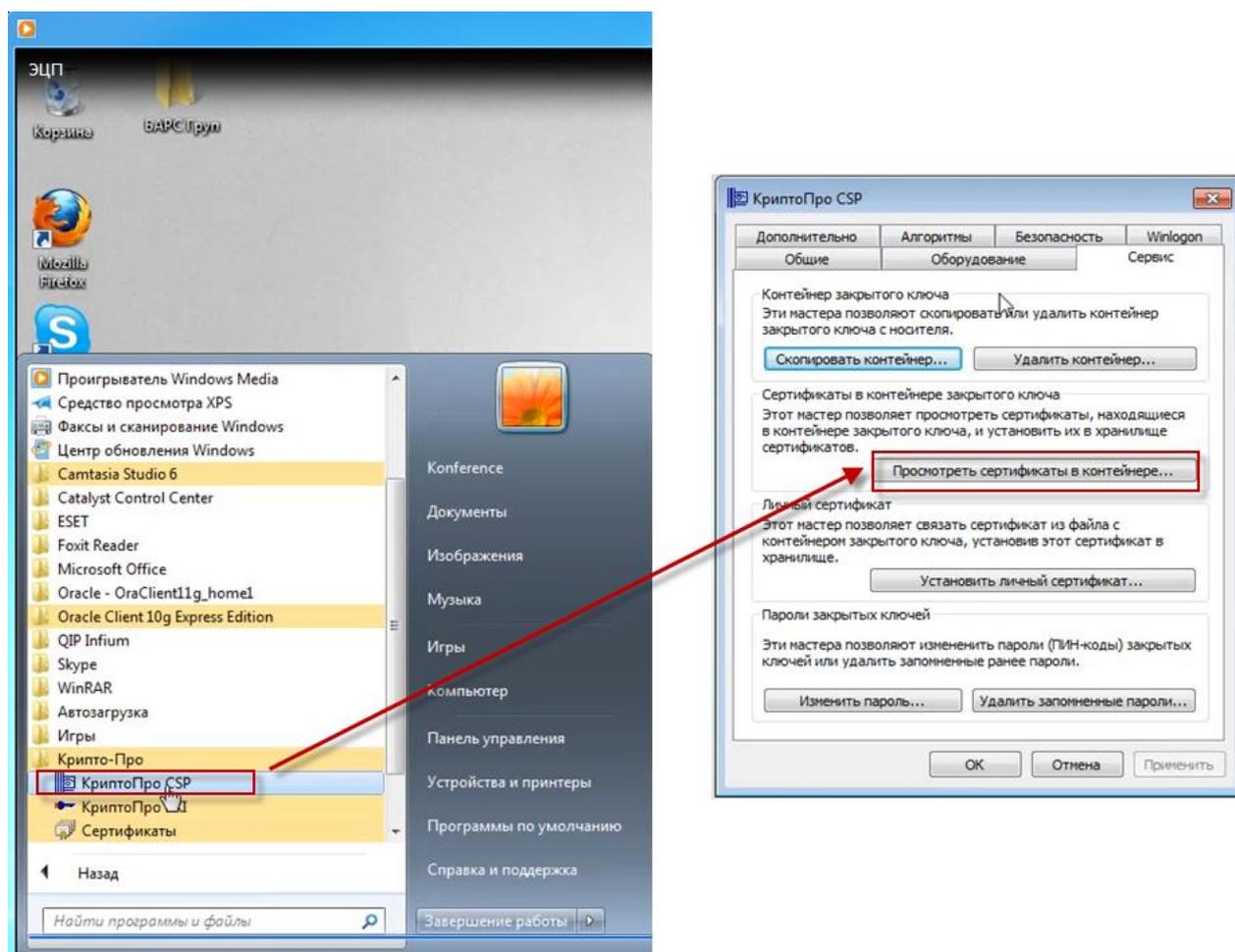


Рисунок 14. Добавление ключа в хранилище

2. В открывшемся диалоговом окне «Сертификаты в контейнере закрытого ключа» нажмите на кнопку «Обзор» и выберите используемый ключ (предварительно установленный в USB-порт или дисковод ключ, предоставленный на носителе ruToken/eToken”) (Рисунок 15). После этого нажмите на кнопку «ОК».

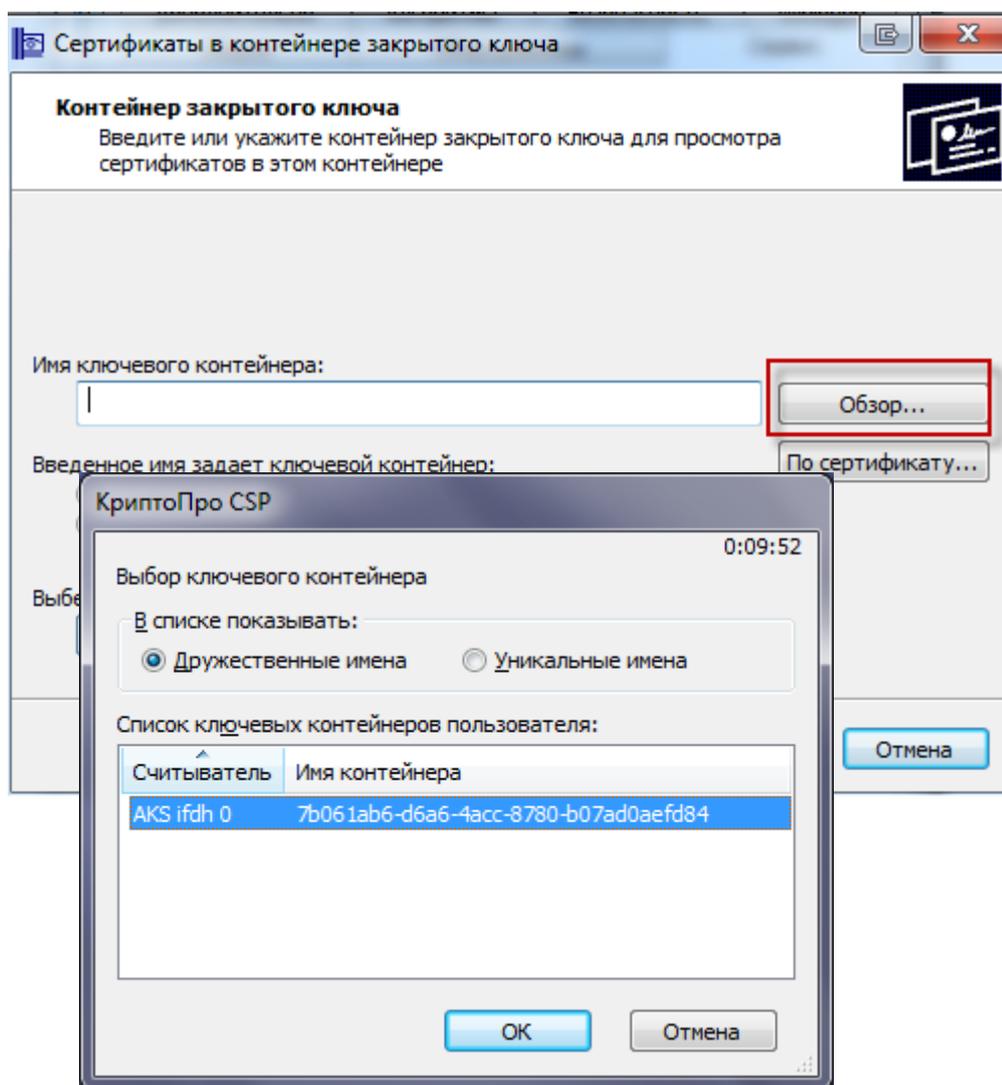


Рисунок 15. Выбор ключевого контейнера

3. Для завершения выбора контейнера закрытого ключа нажмите кнопку «Далее» (Рисунок 16)

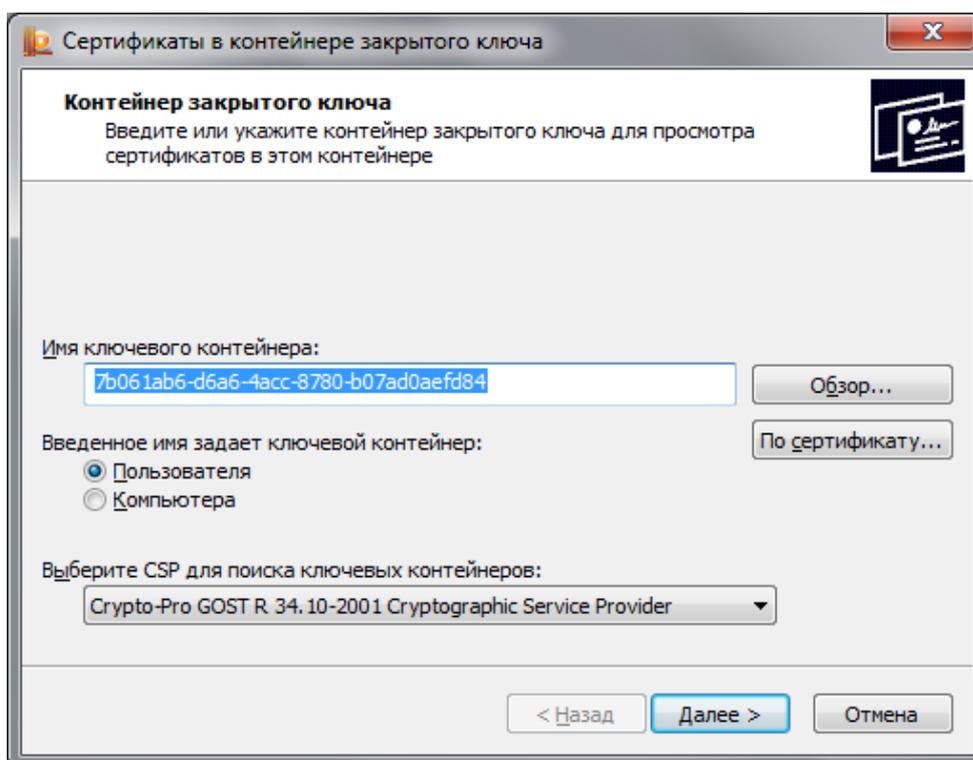


Рисунок 16. Выбор контейнера закрытого ключа

4. В открывшемся диалоговом окне нажмите на кнопку «Установить» (Рисунок 17):

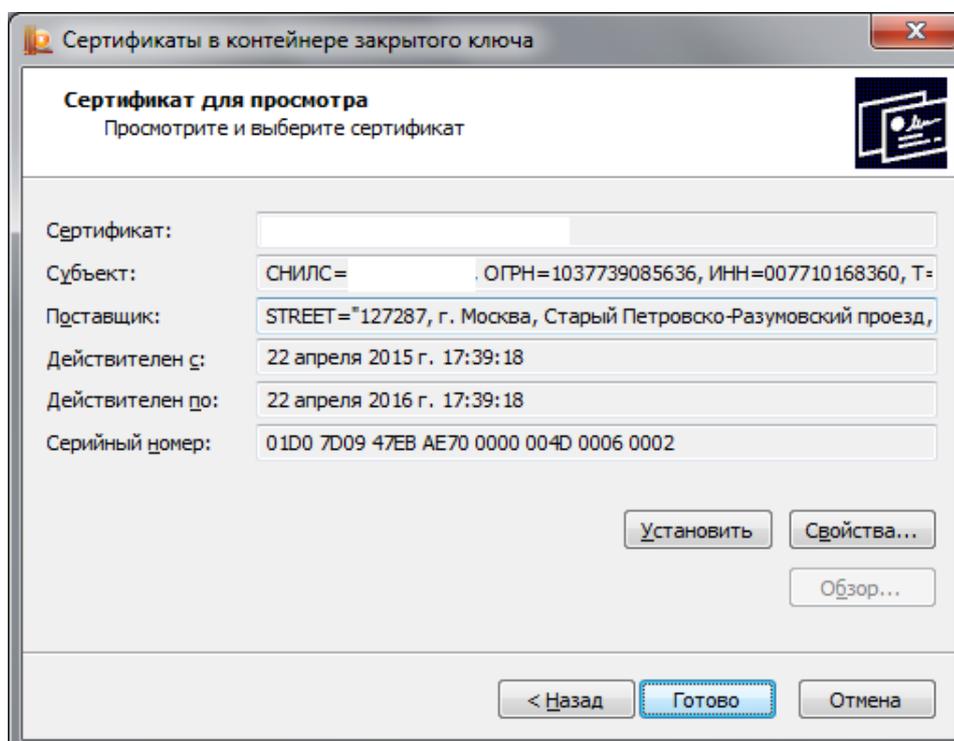


Рисунок 17. Выбор сертификата

5. После установки появится уведомление об успешной установке сертификата. Для подтверждения нажмите кнопку «ОК» (Рисунок 18).

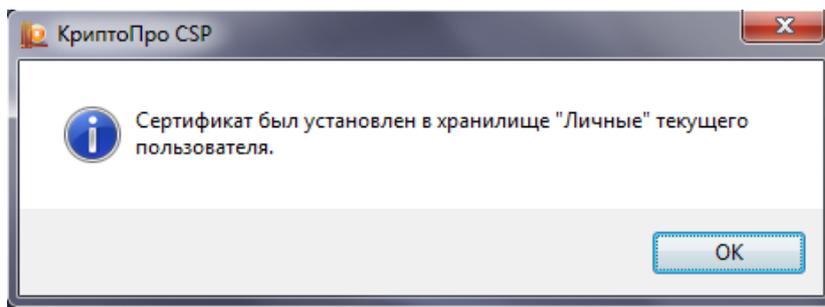


Рисунок 18. Уведомление об успешной установке сертификата

Если в процессе выполнения действий появится сообщение «A new certificate was added to the certificate store» (Рисунок 19), необходимо нажать кнопку «Cancel».

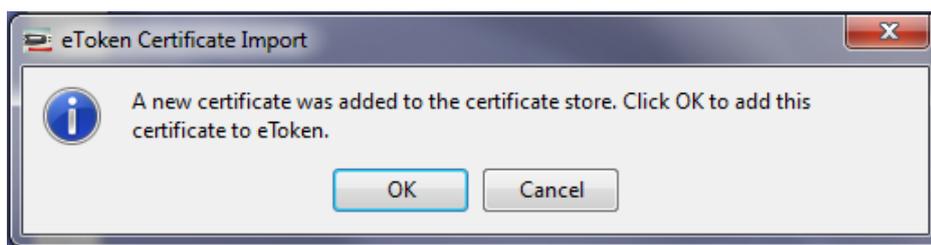


Рисунок 19. Сообщение драйвера eToken

6. Для установки сертификата доверенного корневого центра сертификации нажмите кнопку «Свойства» в окне выбора сертификата (Рисунок 17).

7. В открывшемся окне перейдите на вкладку «Путь сертификации» (Рисунок 20).

8. Проверьте, установлен ли сертификат верхнего уровня (сертификат доверенного корневого центра сертификации).

Знак (1)  свидетельствует о том, что сертификат не установлен.

Знак (2)  свидетельствует о том, что сертификат установлен.

Если у первого в списке сертификата стоит знак 1, то нажатием левой кнопки мыши выберите данный сертификат.

Если у первого в списке сертификата стоит знак 2, переходите к шагу 22 раздела 1.3.2 данной инструкции.

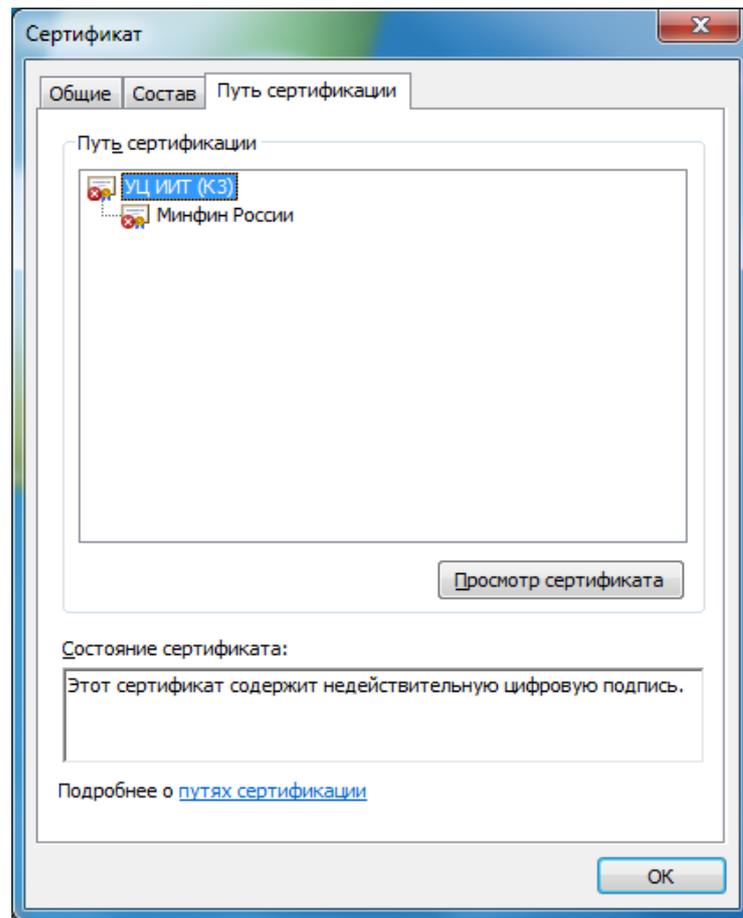


Рисунок 20. Сертификат. Путь сертификации

9. После выбора сертификата, нажмите на кнопку «Просмотр сертификата». В открывшемся окне перейдите на вкладку «Состав» и нажмите на кнопку «Копировать в файл...» (Рисунок 21)

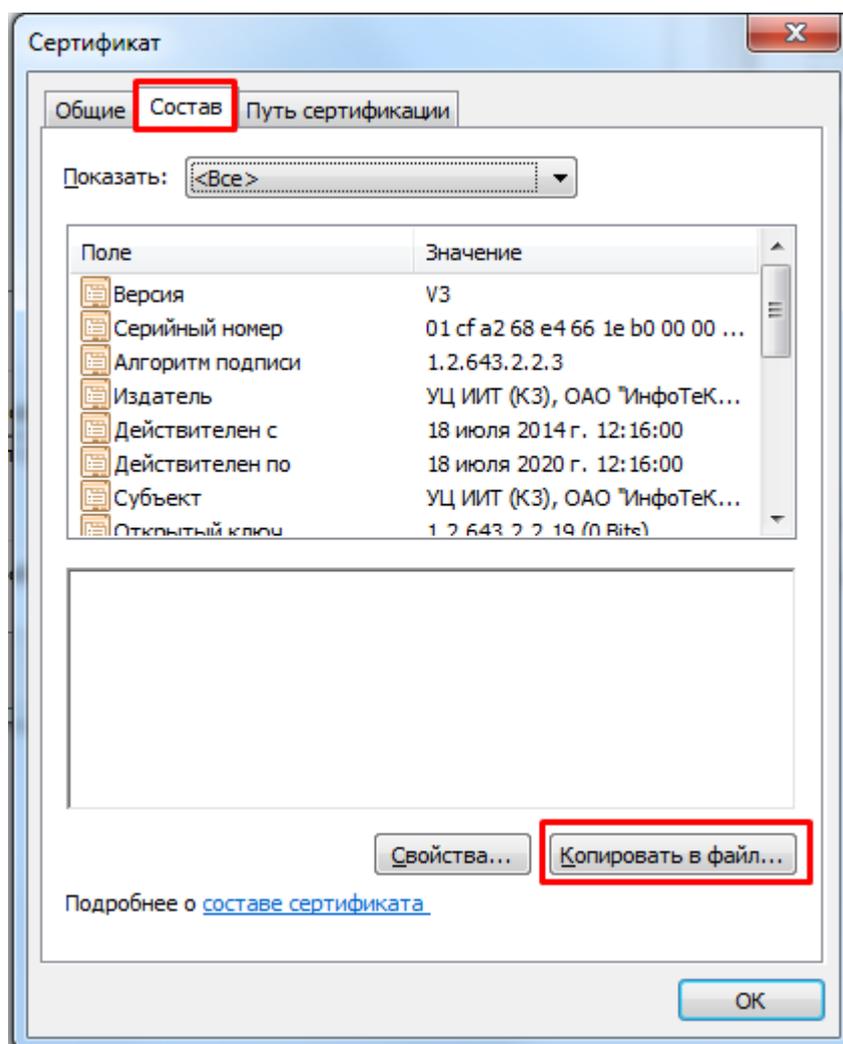


Рисунок 21. Копирование сертификата в файл

10. В открывшемся мастере экспорта сертификатов нажмите на кнопку «Далее».

11. Убедитесь, что в открывшемся окне выбора формата экспортируемого сертификата выбран только вариант «Файлы X.509 (.CER) в кодировке DER», затем нажмите кнопку «Далее».

12. В окне «Имя экспортируемого файла» нажмите кнопку «Обзор».

13. В диалоговом окне «Сохранить как» перейдите в папку «Рабочий стол», в поле «Имя файла» укажите «Сертификат для ЭБ», нажмите кнопку «Сохранить».

14. Убедитесь, что в окне «Имя экспортируемого файла» в поле «Имя файла» верно отобразился путь сохранения сертификата (например, C:\Users\0990\Desktop\Сертификат для ЭБ.cer). Нажмите кнопку «Далее».

15. Подтвердите успешный экспорт сертификата, нажав кнопку «ОК».

16. В окне «Завершение работы мастера экспорта сертификатов» нажмите кнопку «Готово»

17. Перейдите в папку «Рабочий стол», найдите и откройте файл «Сертификат для ЭБ.сег».

18. В появившемся окне нажмите на кнопку «Установить сертификат» (Рисунок 22). На экране отобразится мастер импорта сертификатов, где необходимо нажать кнопку «Далее».

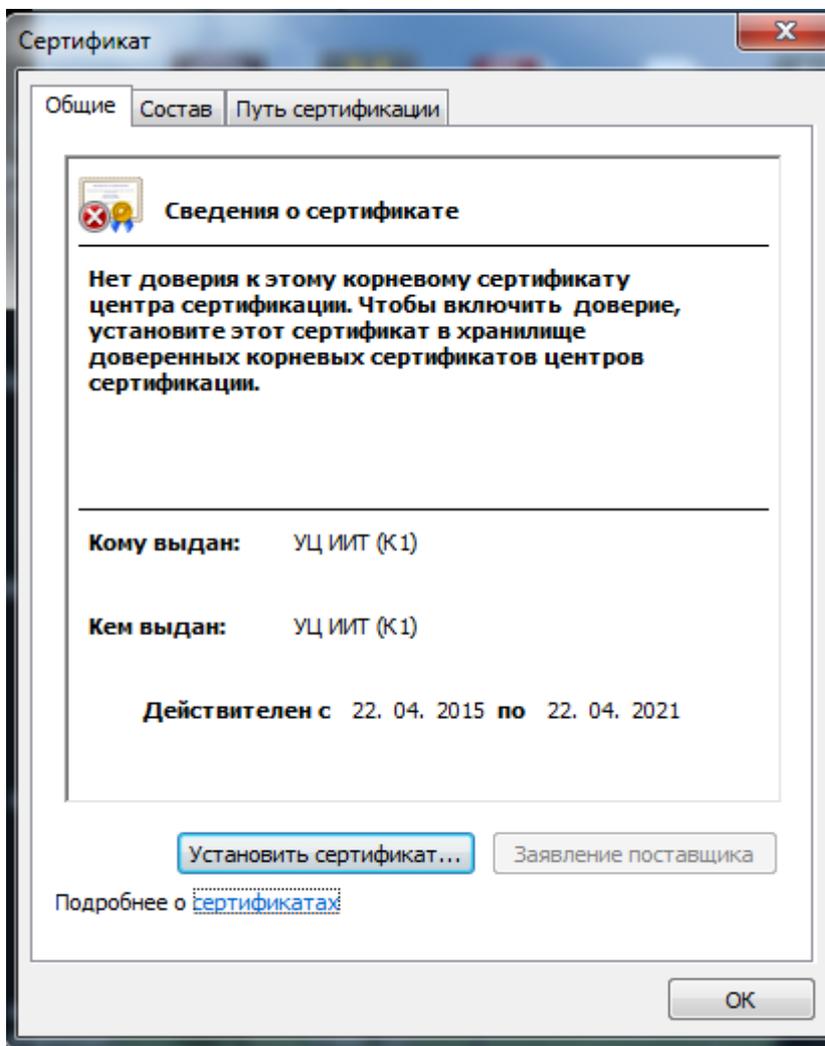


Рисунок 22. Установка корневого сертификата центра сертификации

19. В окне «Хранилище сертификата» (Рисунок 23) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище». Нажать кнопку «Обзор...».

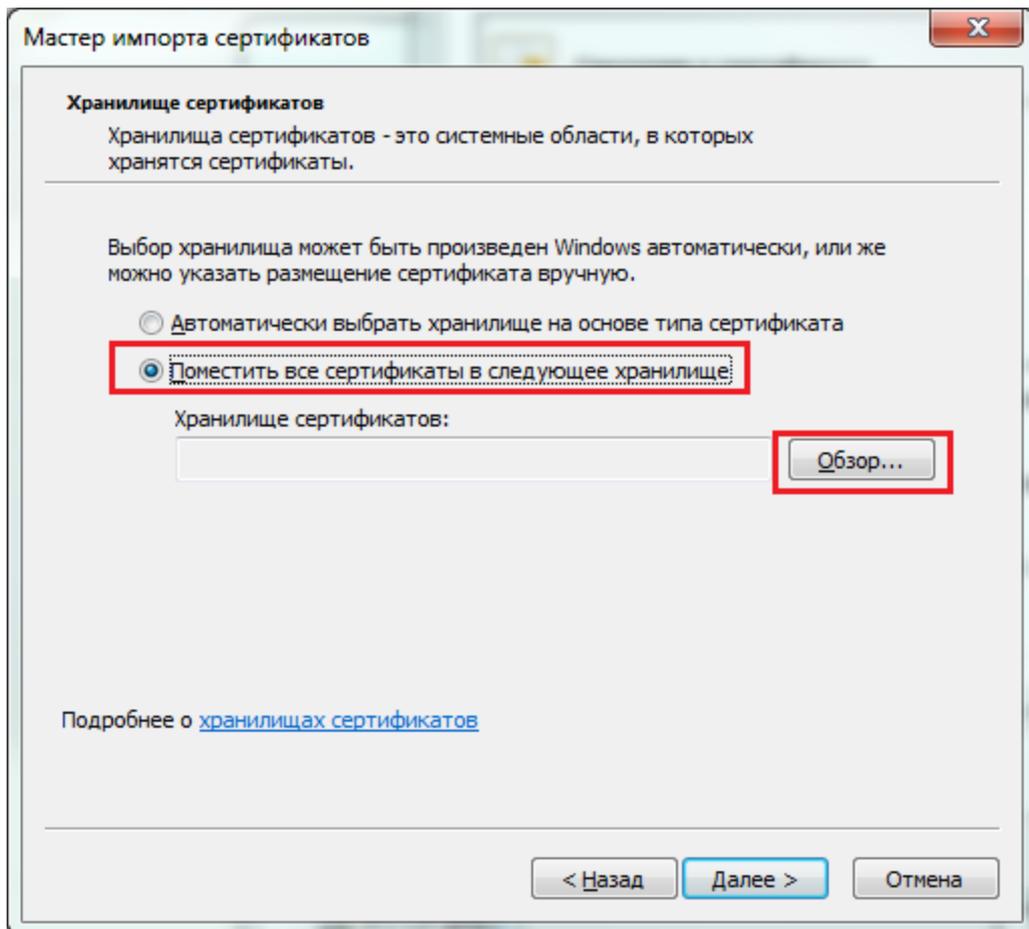


Рисунок 23. Выбор хранилища сертификата

20. В окне выбора хранилища сертификатов выберите контейнер «Доверенные корневые центры сертификации». Нажмите кнопку «Ок» (**Ошибка! Источник ссылки не найден.**).

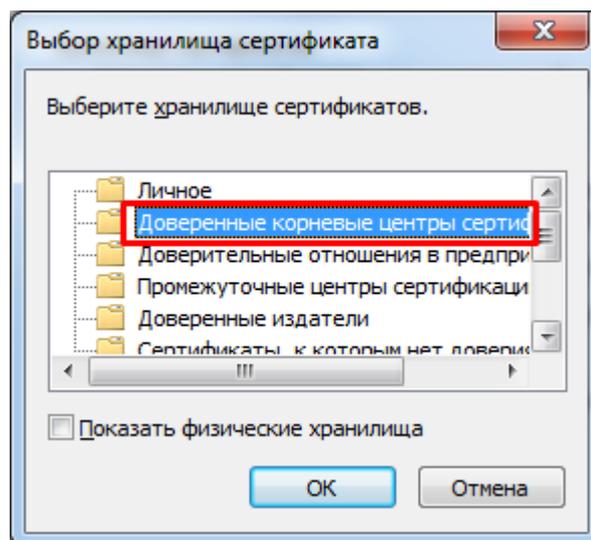


Рисунок 24. Выбор хранилища сертификата

21. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее» затем кнопку «Готово». В случае успешного импорта сертификата отобразится диалог

«Импорт успешно выполнен», где необходимо нажать кнопку «ОК». Если появится окно «Предупреждение безопасности» нажмите кнопку «Да».

22. Убедитесь, что личный сертификат с наименованием, аналогичным тому, что было указано в поле «Сертификат» на Рисунок 17, успешно установлен в директории «Сертификаты–текущий пользователь – Личное – Реестр – Сертификаты». Для этого запустите утилиту «Сертификаты» расположенную в «Пуск/Все программы/КриптоПро/Сертификаты» и найдите данный сертификат в директории «Сертификаты–текущий пользователь – Личное – Реестр – Сертификаты» (Рисунок 25).

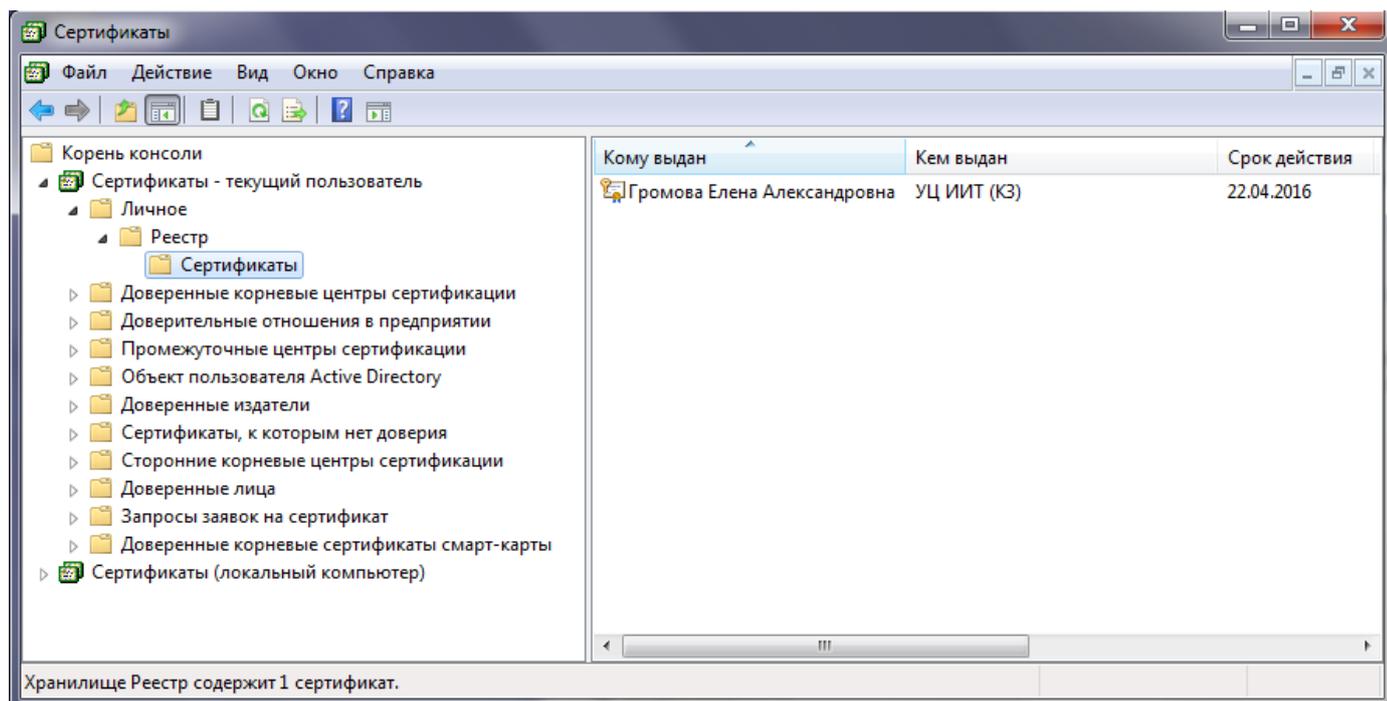


Рисунок 25. Утилита «Сертификаты»

23. Если сертификат отсутствует, вернитесь к шагу 4, нажмите кнопку «Свойства» и установите сертификат, следуя шагам 18-21 раздела 1.3.2 данной инструкции, выбрав на шаге 20 контейнер «Личное».

24. Если сертификат присутствует, откройте его. Перейдите на вкладку «Путь сертификации» и проверьте, установлен ли сертификат доверенного корневого центра сертификации в соответствии с шагом 8 раздела 1.3.2 данной инструкции. Если сертификат установлен, то автоматизированное рабочее место пользователя успешно настроено для работы с Системой.

1.3.4. Настройка Internet Explorer

1. Открыть свойства веб-обозревателя Internet Explorer.
2. Перейти на вкладку «Безопасность».

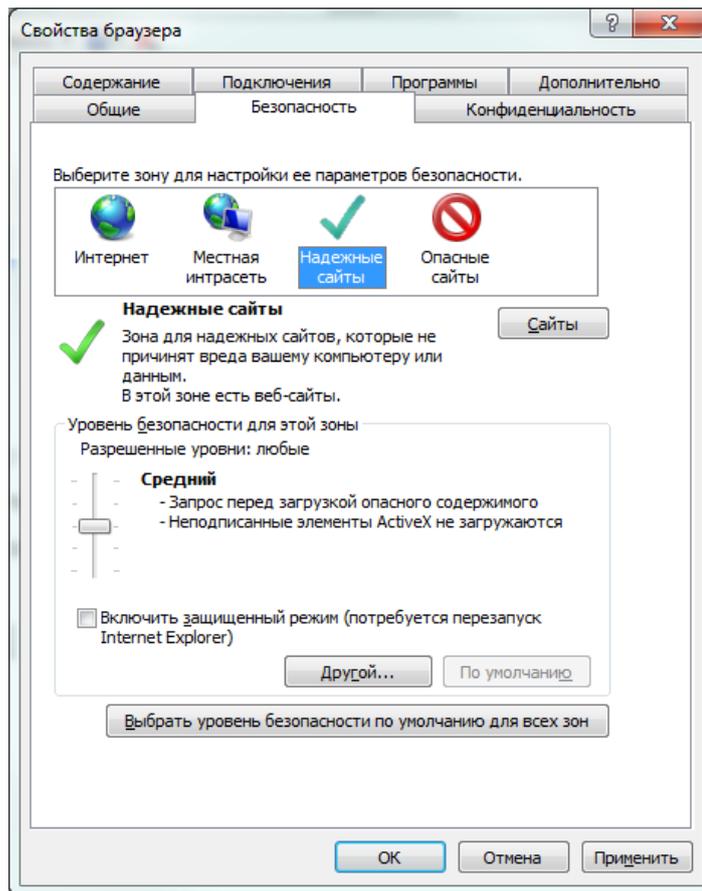


Рисунок 26. Диалог настройки безопасности браузера

3. Выбрать зону для настройки «Надежные узлы» (Рисунок 26).
4. Нажать кнопку «Сайты».

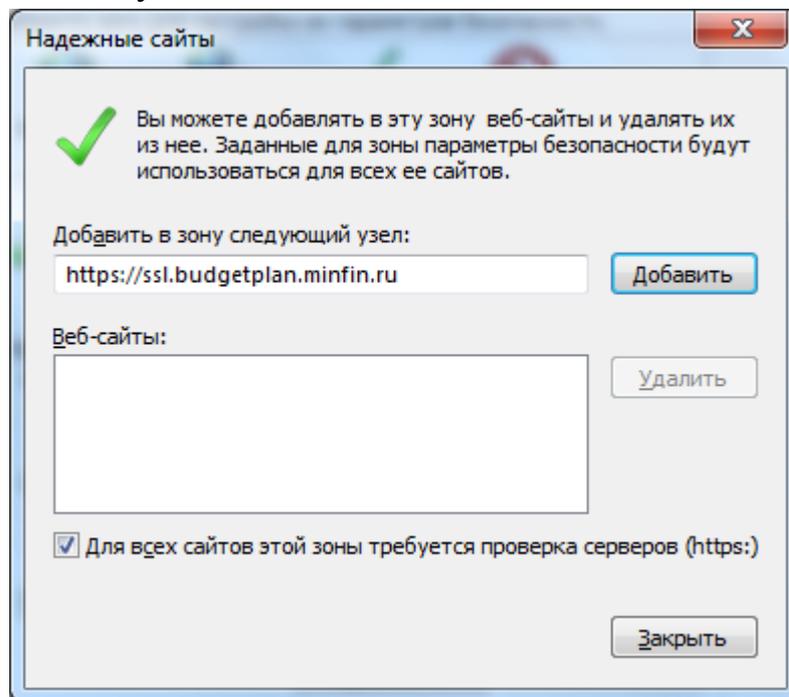


Рисунок 27. Диалог настройки доверенных узлов.

5. В поле «Добавить в зону следующий узел» задать значение «https://ssl.budgetplan.minfin.ru/» и нажать кнопку «Добавить» (Рисунок 27).

6. В окне «Надежные сайты» нажать кнопку «Закреть».
7. В окне «Свойства браузера» нажать кнопку «ОК».

2. ВХОД ПОДСИСТЕМУ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ «ЭЛЕКТРОННЫЙ БЮДЖЕТ»

1. Для входа в Систему необходимо запустить интернет браузер «Internet Explorer» и в адресной строке ввести <http://budget.gov.ru/lk> (Рисунок 28).

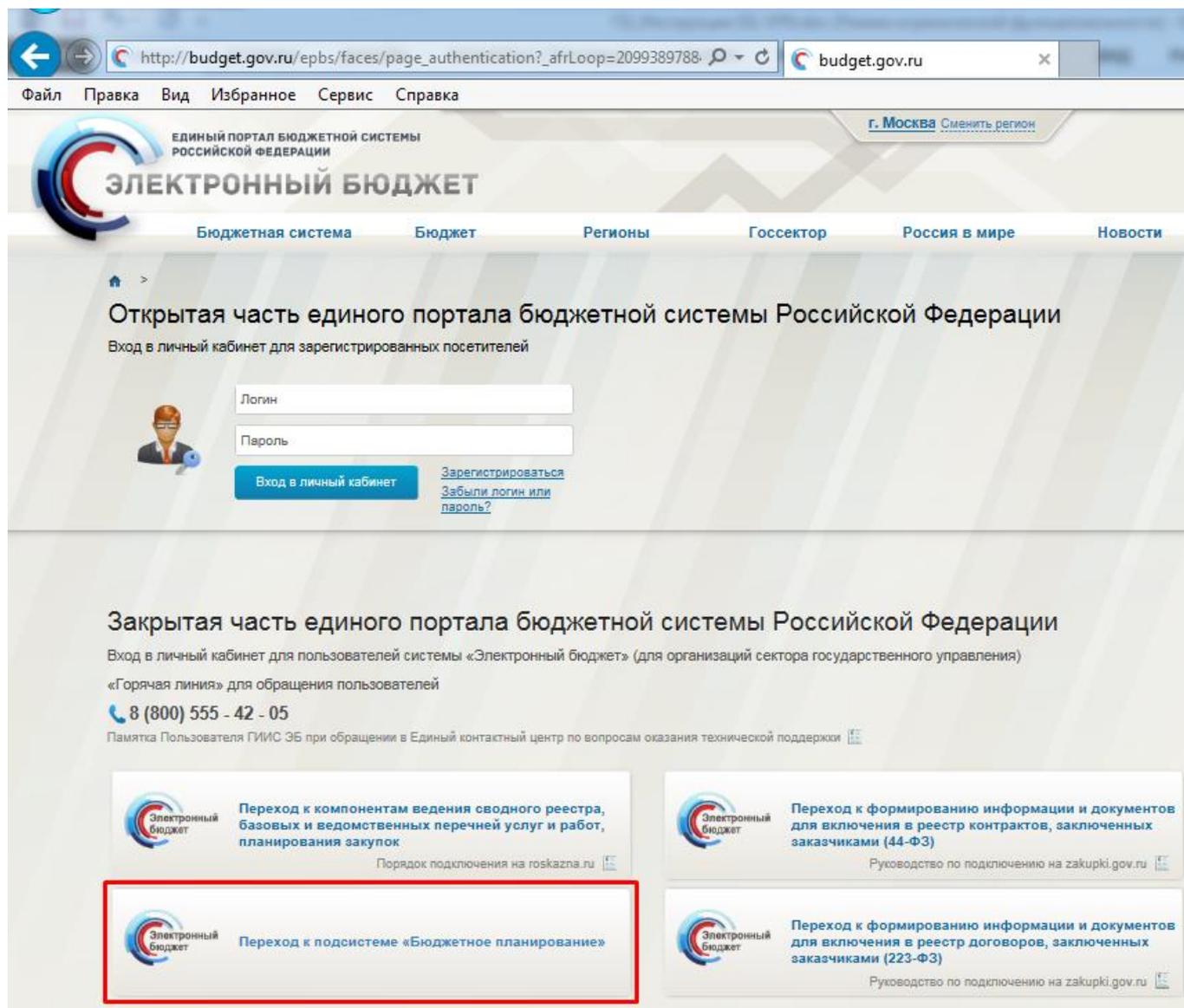


Рисунок 28. Единый портал бюджетной системы

2. На странице Единого портала бюджетной системы нажмите на кнопку «Переход к подсистеме «Бюджетное планирование»».

3. После нажатия на кнопку браузер осуществит перенаправление по адресу <https://ssl.budgetplan.minfin.ru/http/BudgetPlan/> . Если перенаправление не произошло, введите указанную ссылку в адресную строку браузера.

4. В появившемся окне, нажмите на кнопку «Вход по сертификату» (Рисунок 29).

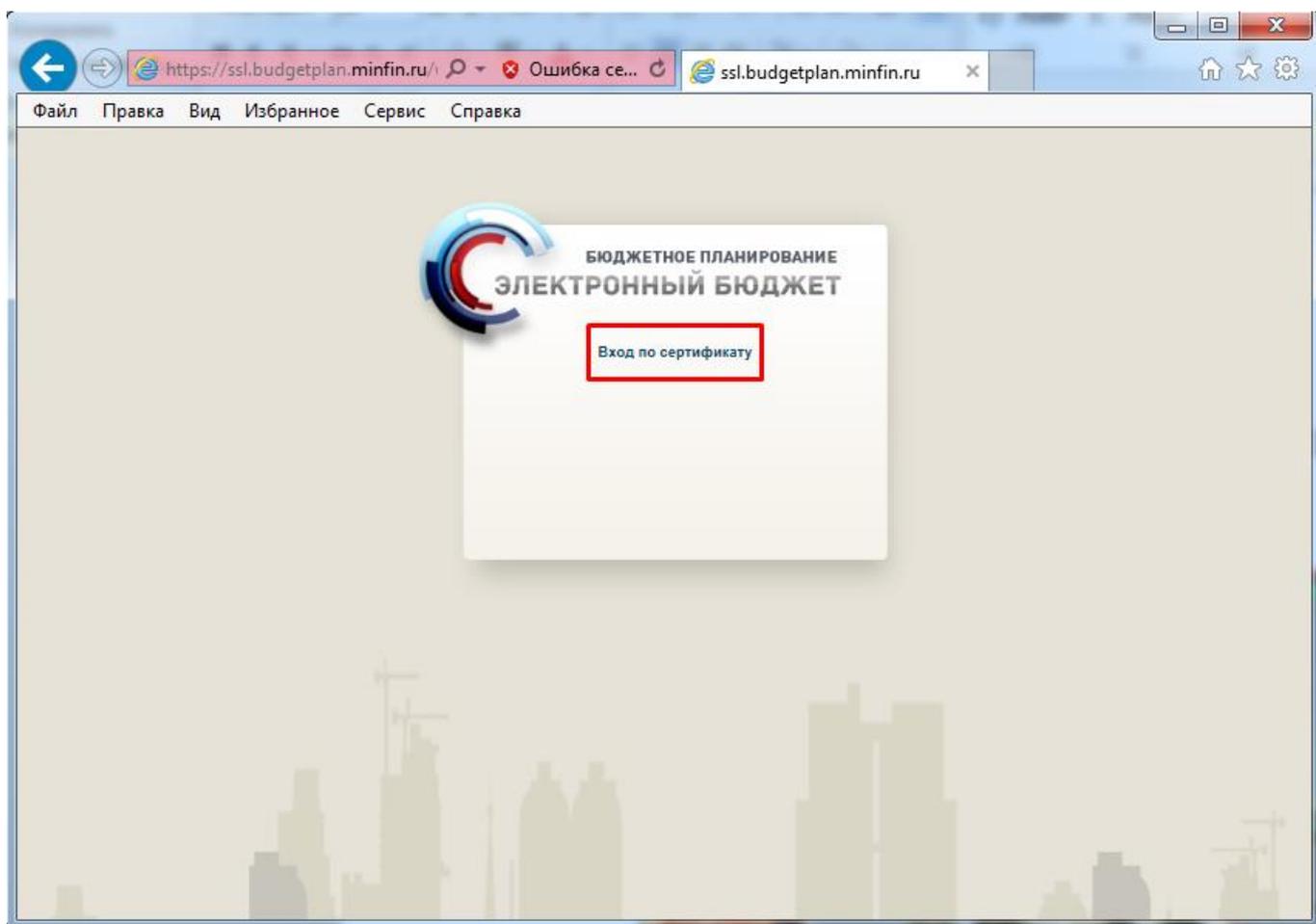


Рисунок 29. Окно выбора вида входа в систему

5. После выбора метода аутентификации «Вход по сертификату», Система автоматически запрашивается сертификат ключа проверки электронной подписи и пин-код сертификата, затем осуществляется поиск пользователя-владельца сертификата и происходит открытие главного окна Системы.

Если различные пользователи используют для авторизации один сертификат (например, одно уполномоченное лицо имеет различные роли), то Система предложит выбрать конкретного пользователя (Рисунок 30). После выбора логина, необходимо нажать кнопку «Войти».

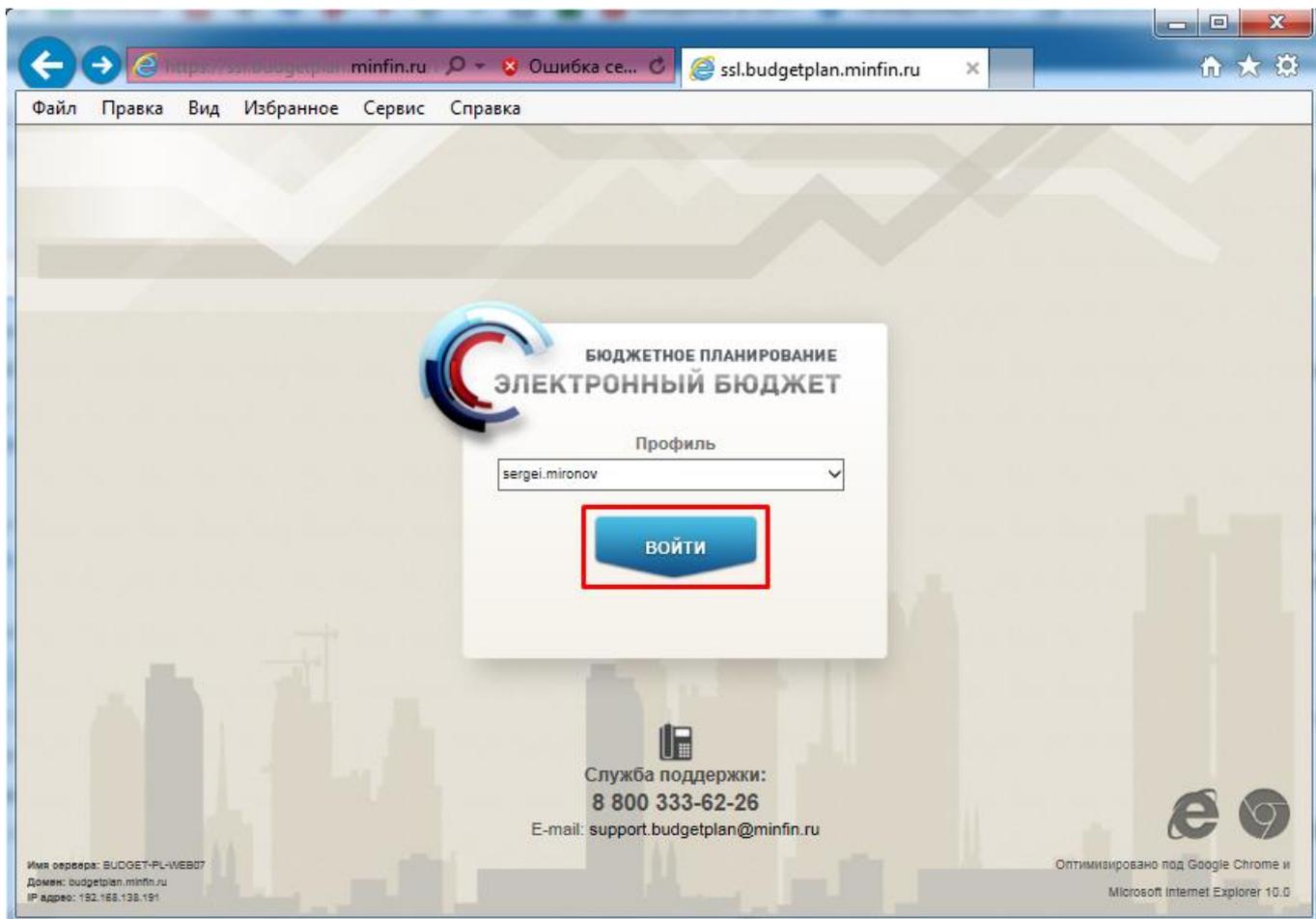


Рисунок 30. Окно выбора логина пользователя

3. ПРОБЛЕМЫ ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ И ИХ УСТРАНЕНИЕ

3.1. Проблема с сертификатом безопасности

Если между шагами 3 и 4 раздела 2 данной инструкции появляется сообщение «Возникла проблема с сертификатом безопасности этого веб-сайта» (Рисунок 31), необходимо нажать на кнопку «Продолжить открытие веб-сайта (не рекомендуется)».



Рисунок 31. Проблема с сертификатом безопасности

3.2. Вставьте ключевой носитель

Если между шагами 3 и 4 раздела 2 данной инструкции появляется сообщение КриптоПРО CSP «Вставьте ключевой носитель» (Рисунок 32), необходимо:

1. Установить установите в рабочий USB-порт автоматизированного рабочего места пользователя Системы, предоставленный на носителе ruToken/eToken.
2. Перезапустите браузер Internet Explorer.
3. Повторите шаги раздела 2 данной инструкции.

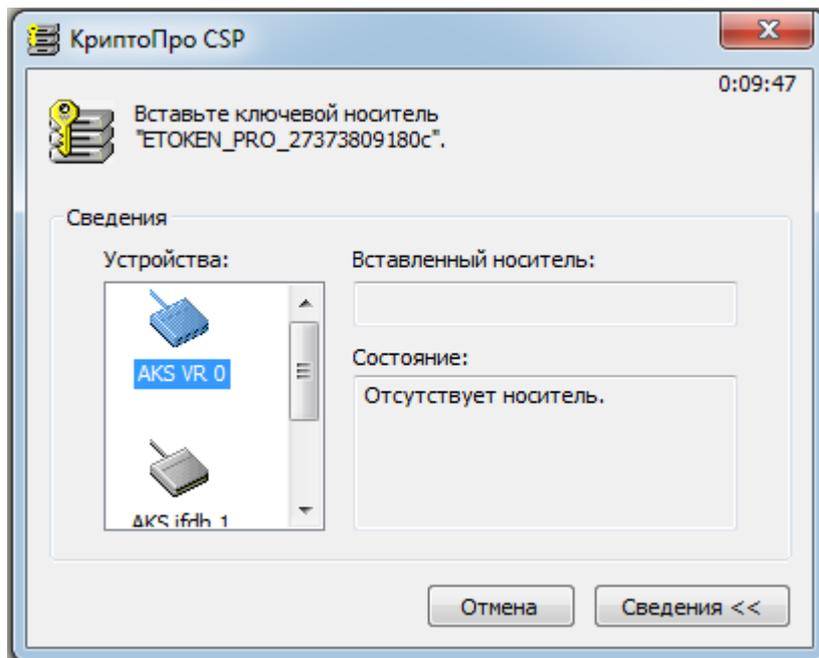


Рисунок 32. Вставьте ключевой носитель

3.3. Не удается отобразить эту страницу

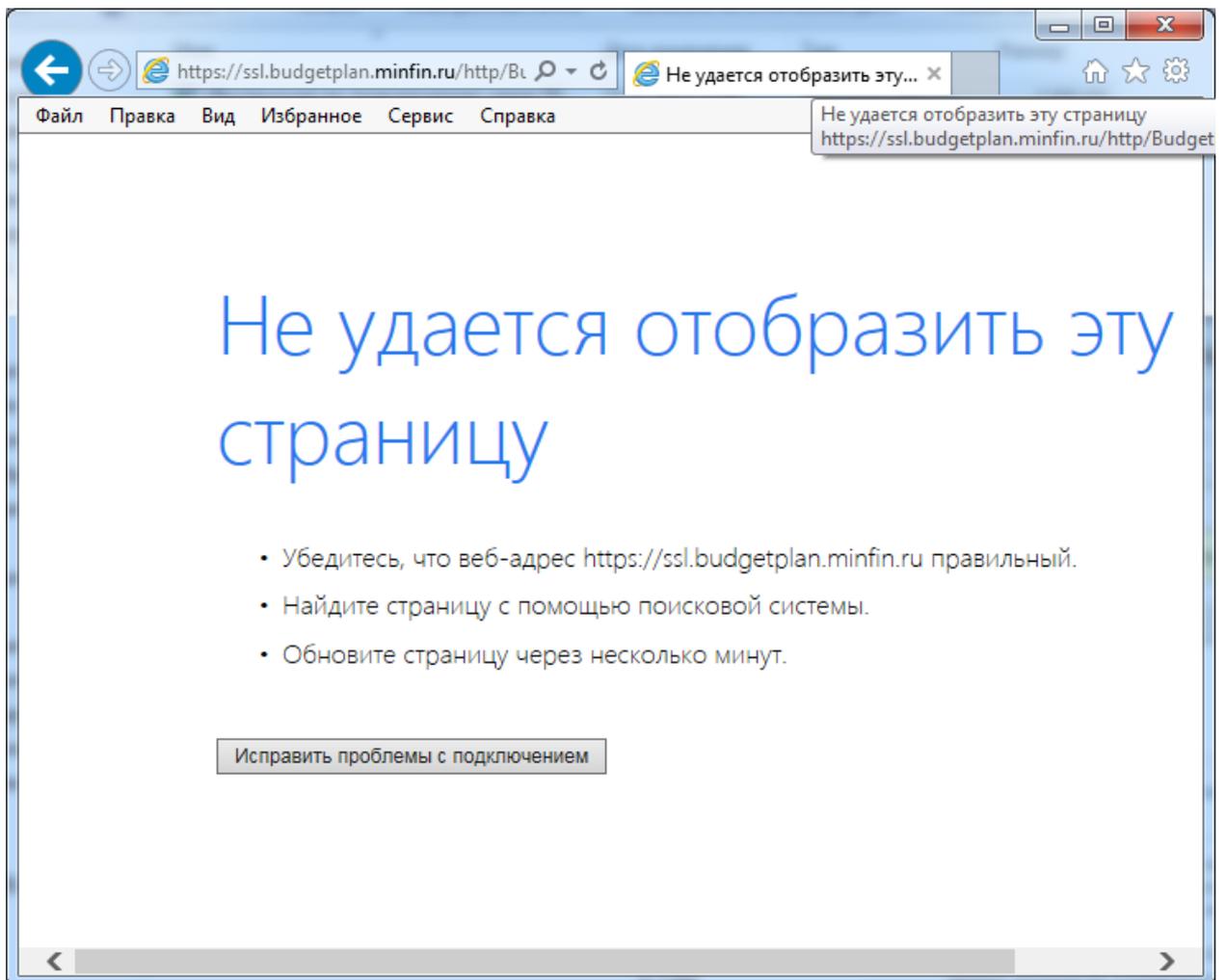


Рисунок 33. Не удается отобразить эту страницу

Если появляется сообщение об ошибке «Не удастся отобразить эту страницу» (Рисунок 33), необходимо:

1. Проверить версию браузера Internet Explorer (версия должна быть не ниже Internet Explorer 10) при необходимости обновите. Для проверки версии:
откройте браузер Internet Explorer;
в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 34) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.

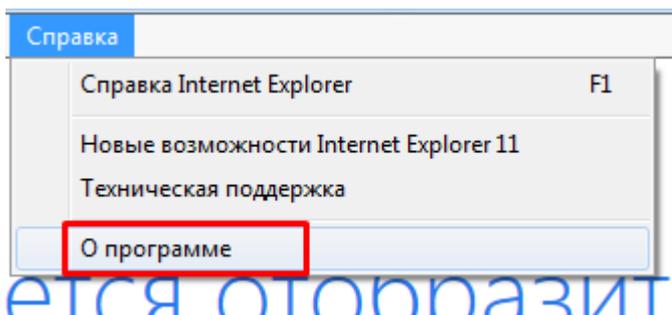


Рисунок 34. О программе

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установить (см. раздел 1.3.1. данной инструкции).
3. Проверить настройки «КриптоПРО CSP» (см. шаг 3. раздела 1.3.1. данной инструкции).

3.4. 403 Access Denied

В случае возникновения ошибки «403 Access Denied» (Рисунок 35), необходимо в соответствии с шагами 6-17 раздела 1.3.3. данной инструкции сохранить сертификат корневого центра сертификации, заархивировать его (**обязательно!**) и отправить его на адрес электронной почты 0990@minfin.ru с указанием, наименования учреждения, ФИО пользователя и логина в Системе.

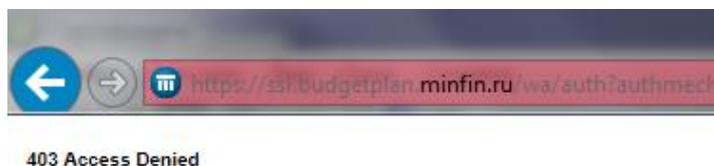


Рисунок 35. 403 Access Denied

3.5. Не удается отобразить эту страницу. Включите протоколы TLS

Если появляется сообщение об ошибке «Не удастся отобразить эту страницу» (Рисунок 36), необходимо:



Не удастся отобразить эту страницу

Включите протоколы TLS 1.0, TLS 1.1 и TLS 1.2 в разделе "Дополнительные параметры" и снова попробуйте подключиться к веб-странице <https://ssl.budgetplan.minfin.ru>. Если не удастся устранить ошибку, обратитесь к администратору веб-сайта.

Изменить параметры

Рисунок 36. Не удастся отобразить эту страницу. Включите протоколы TLS

1. Проверить версию браузера Internet Explorer (версия должна быть не ниже Internet Explorer 10) при необходимости обновите. Для проверки версии:
откройте браузер Internet Explorer;
в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 34) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.

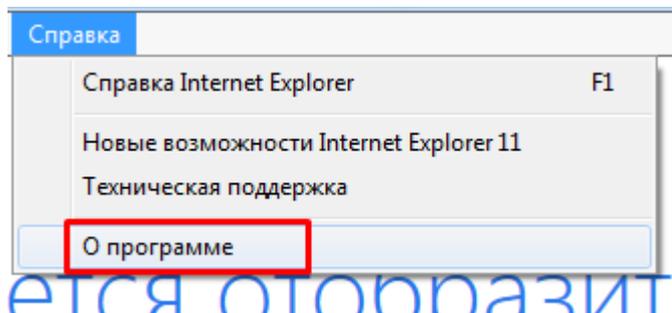


Рисунок 37. О программе

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установить (см. раздел 1.3.1. данной инструкции).
3. Проверить настройки «КриптоПРО CSP» (см. шаг 3. раздела 1.3.1. данной инструкции).
4. Проверить настройки браузера Internet Explorer. Для проверки настроек браузера:
откройте браузер Internet Explorer;
в меню «Сервис» нажмите левой клавишей мыши на кнопку «Свойства браузера» или «Свойства обозревателя»;

в появившемся окне откройте вкладку «Дополнительно» и сверьте настройки с Рисунок 38.

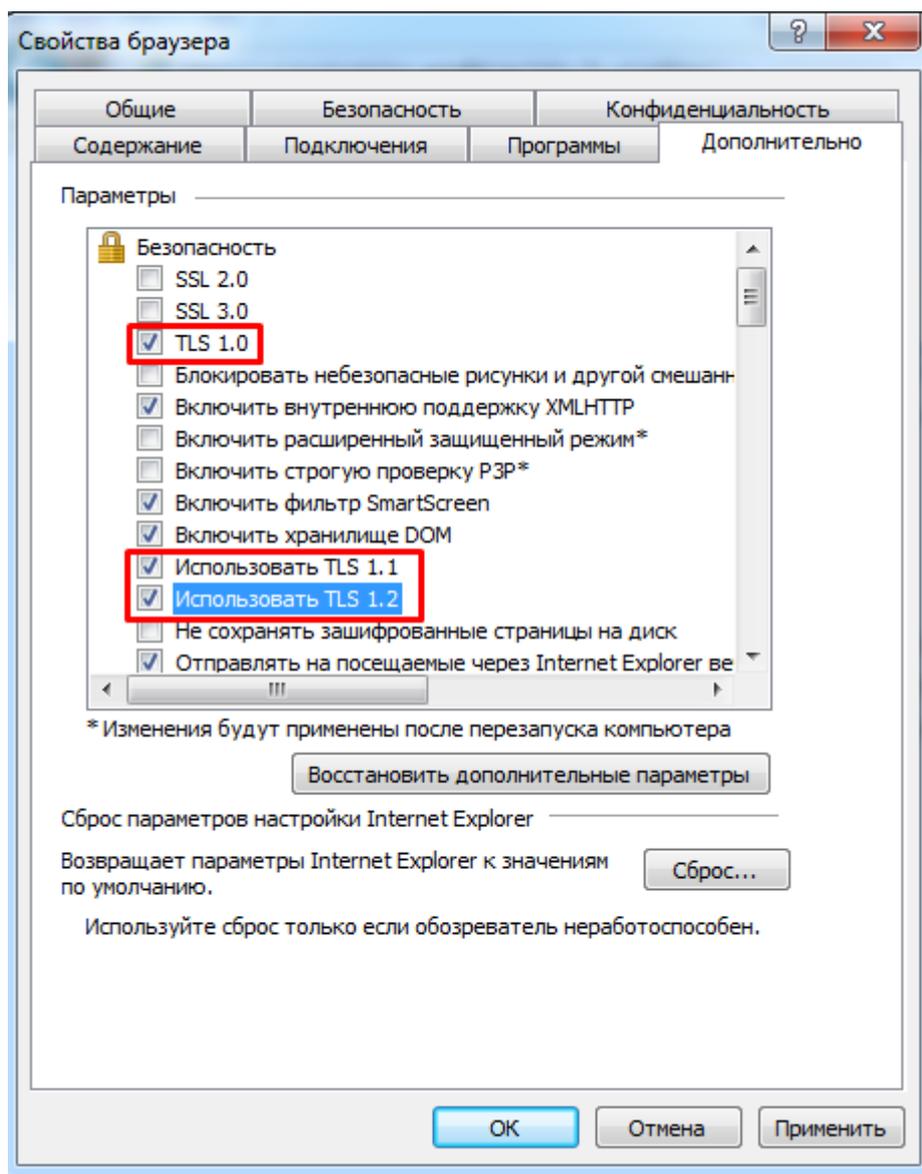


Рисунок 38. Вкладка "Дополнительно"

3.6. Иные ошибки

В случае возникновения ошибок в процессе подключения и настройки программного обеспечения, не описанных в данной инструкции, необходимо:

сделать снимок экрана (скриншот) ошибки;

в соответствии с шагами 6-17 раздела 1.3.3. инструкции сохранить сертификат корневого центра сертификации;

заархивировать (**обязательно!**) сертификат и скриншот;

отправить архив на адрес электронной почты 0990@minfin.ru с указанием, наименования учреждения, ФИО пользователя, логина в Системе и действий, которые привели к ошибке.

При возникновении вопросов, связанных с функционированием Системы необходимо обращаться по телефону: 8 800 333-62-26 или по электронной почте support.budgetplan@minfin.ru.