

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

МОСКВА

2019

Версия от 05.04.18 г.

## **АННОТАЦИЯ**

Настоящий документ является инструкцией по защищенному удаленному подключению пользователей к подсистеме бюджетного планирования и подсистеме управления национальными проектами государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет» (далее – Система) с использованием квалифицированного сертификата ключа проверки электронной подписи (далее – сертификат).

## 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. Требования к сертификату.....	4
1.4. Настройка программного обеспечения .....	5
1.4.1. Установка криптопровайдера «криптопро csp».....	5
1.4.2. Установка и настройка криптопро эцп browser plug-in.....	7
1.4.3. Установка драйвера используемого носителя ключевой информации сертификата пользователя .....	9
1.4.4. Установка личного сертификата и сертификата доверенного корневого центра сертификации .....	15
1.4.5. Настройка Internet Explorer .....	23
1.4.6. Установка корневого сертификата удостоверяющего центра минфина россии .....	25
2. Вход подсистему бюджетного планирования государственной интегрированной информационной системы управления общественными финансами «электронный бюджет» .....	26
3. Проблемы при подключении к системе и их устранение .....	29
3.1. Проблема с сертификатом безопасности .....	29
3.2. Вставьте ключевой носитель.....	29
3.3. Не удается отобразить эту страницу.....	30
3.4. Окно ввода логина и пароля .....	31
3.5. Не удается отобразить эту страницу. Включите протоколы tls .....	32
3.6. Иные ошибки .....	33

## **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 1,2 МГц, не менее 2 ядер.
- 2) Объем оперативной памяти, не менее 2048 Мб;
- 3) Объем жесткого диска, не менее 50 Гб;
- 4) Клавиатура, манипулятор типа мышь;
- 5) Монитор SVGA (графический режим должен иметь разрешение не менее 1024x768);
- 6) USB-порт;
- 7) Квалифицированный сертификат ключа проверки электронной подписи.

На рабочем месте должен быть предоставлен доступ к сети Интернет со скоростью не менее 10 Мбит/сек.

### **1.2. Требования к программному обеспечению**

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

- 1) Интернет-браузер «Internet Explorer» версия 11 и выше, интернет-браузер «Спутник» или «Яндекс.Браузер» с поддержкой отечественной криптографии;
- 2) Операционная система: Windows Vista/7/8/8.1/10, Astra Linux Special Edition, Astra Linux Common Edition (x64), ALT Linux 6/7 (x86, x64, ARM), Альт Сервер 8, Альт Рабочая станция 8, Альт Рабочая станция К 8 (x86, x64, ARM, ARM64).

Сертифицированная версия «КриптоПро CSP» версия 4.0 и выше (в связи с переходом на ГОСТ Р 34.10-2012)

- 3) КриптоПро ЭЦП Browser plug-in версия 2.0 и выше

### **1.3. Требования к сертификату**

Для утверждения (подписания) документов в Системе подходит любой, выданный аккредитованным УЦ, сертификат юридического лица с указанием физического лица (владельца сертификата), действующего от имени юридического лица на основании учредительных документов или доверенности.

В соответствии с Приказом ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» сертификат юридического лица должен содержать:

уникальный номер квалифицированного сертификата;  
даты начала и окончания действия квалифицированного сертификата;  
наименование и место юридического лица, а также в случаях, предусмотренных Федеральным законом, фамилия, имя и отчество (если имеется) физического лица, действующего от имени владельца квалифицированного сертификата - юридического лица на основании учредительных документов юридического лица или доверенности;

основной государственный регистрационный номер (далее - ОГРН) юридического лица - владельца квалифицированного сертификата;

идентификационный номер налогоплательщика (далее - ИНН) юридического лица - владельца квалифицированного сертификата;

ключ проверки ЭП;

наименование используемого средства ЭП и (или) стандарты, требованиям которых соответствует ключ ЭП и ключ проверки ЭП;

наименования средств ЭП и средств аккредитованного УЦ, которые использованы для создания ключа ЭП, ключа проверки ЭП, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом;

наименование и место нахождения аккредитованного УЦ, который выдал квалифицированный сертификат;

номер квалифицированного сертификата аккредитованного УЦ;

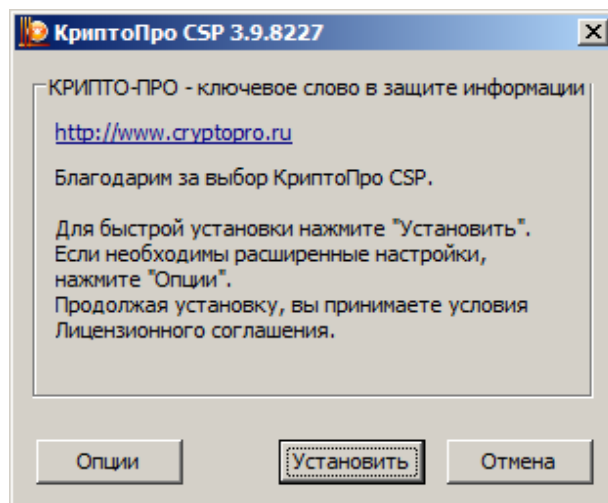
ограничения использования квалифицированного сертификата (если такие ограничения установлены).

Кроме того, для работы в подсистеме бюджетного планирования сертификат должен иметь дополнительное поле СНИЛС (snils), с указанием номера СНИЛС уполномоченного лица – владельца сертификата.

## **1.4. Настройка программного обеспечения**

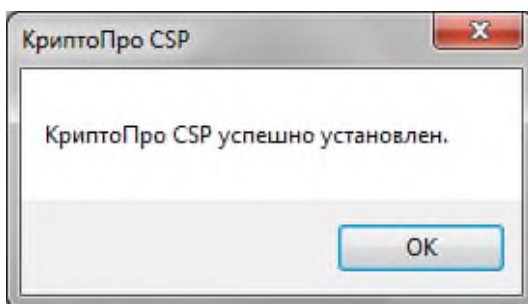
### **1.4.1. Установка криптопровайдера «КриптоПро CSP»**

1. Загрузите и запустите установочный файл сертифицированной версии «КриптоПро CSP», доступный для скачивания по адресу <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).

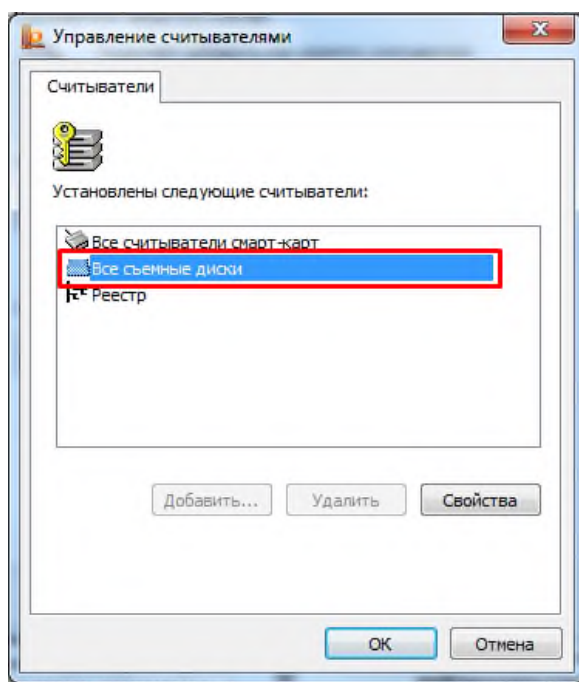


**Рисунок 2. Установка «КриптоПро CSP»**

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

*Возможны проблемы при входе в Систему, в случае, если программа «КриптоПро CSP» не активирована и (или) истек пробный период.*

3. Если в качестве носителя ключевой информации сертификата пользователя используется flash-накопитель или дискета, запустите «КриптоПро CSP» (Пуск/Все программы/КриптоПро/КриптоПро CSP). Откройте вкладку «Оборудование», нажмите кнопку «Настроить считыватели». В появившемся окне, выберите пункт «Все съемные диски» (Рисунок 3).



**Рисунок 3. Настройка считывателей**

4. Нажмите кнопку «Добавить». Если кнопка добавить неактивна, перейдите во вкладку «Общие» и нажмите кнопку «Запустить с правами администратора».

5. В окне «Мастера установки считывателя нажмите кнопку «Далее».

6. В появившемся окне выберите считыватель, соответствующий usb-порту, ключевому носителю на flash –накопителе или дисководу гибких дисков (дискет).

7. В окне «Мастера установки считывателя нажмите кнопку «Далее» и «Готово».

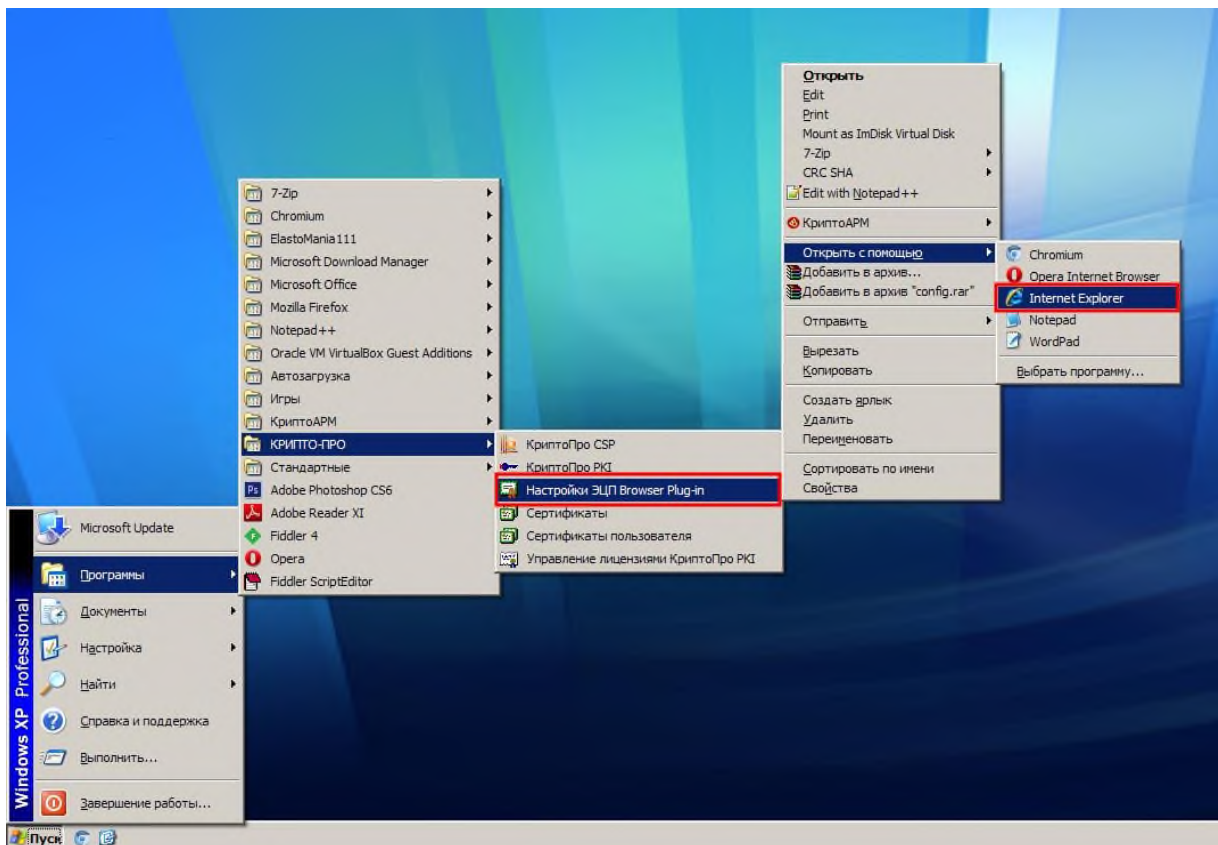
#### **1.4.2. Установка и настройка КриптоПро ЭЦП Browser plug-in**

1. Загрузите и установите «КриптоПро ЭЦП Browser plug-in», доступный для скачивания по адресу <https://www.cryptopro.ru/products/cades/plugin>.

В случае использования интернет-браузеров «Спутник» или «Яндекс.Браузер» с поддержкой отечественной криптографии **дополнительно** необходимо в указанных интернет-браузерах установить расширение «CryptoPro Extension for CAdES Browser Plug-in», доступное в «Интернет-магазине chrome» по адресу <https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnmpdbibifmljnfjhpififfog>

2. Откройте меню «Пуск» - «Все программы» - «КриптоПРО»

3. Откройте ярлык «**Настройки ЭЦП Browser Plug-In**» с использованием интернет-браузера Internet Explorer или иного интернет-браузера установленного в операционной системе по умолчанию (Рисунок 4).



**Рисунок 4. Открытие ярлыка «Настройки ЭЦП Browser Plug-In»**

4. В случае открытия с использованием интернет-браузера «Internet Explorer», интернет-браузер сообщит о блокировке сценария. Разрешите запуск заблокированного содержимого (внешний вид и текст сообщения может варьироваться в зависимости от версии операционной системы и версии интернет-браузера «Internet Explorer») (Рисунок 5).



**Рисунок 5. Предупреждение интернет-браузера «Internet Explorer»**

5. Добавьте узел <https://ssl.budgetplan.minfin.ru/> в поле списка доверенных узлов и нажмите «+», после чего нажмите Сохранить (Рисунок 6)



## Список доверенных узлов

✕ <https://ssl.budgetplan.minfin.ru/>

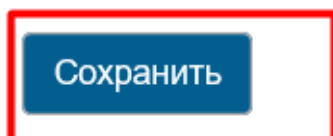
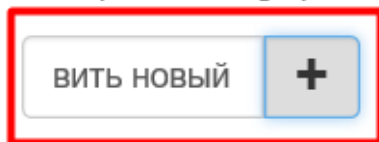


Рисунок 6. Добавление узла в список доверенных

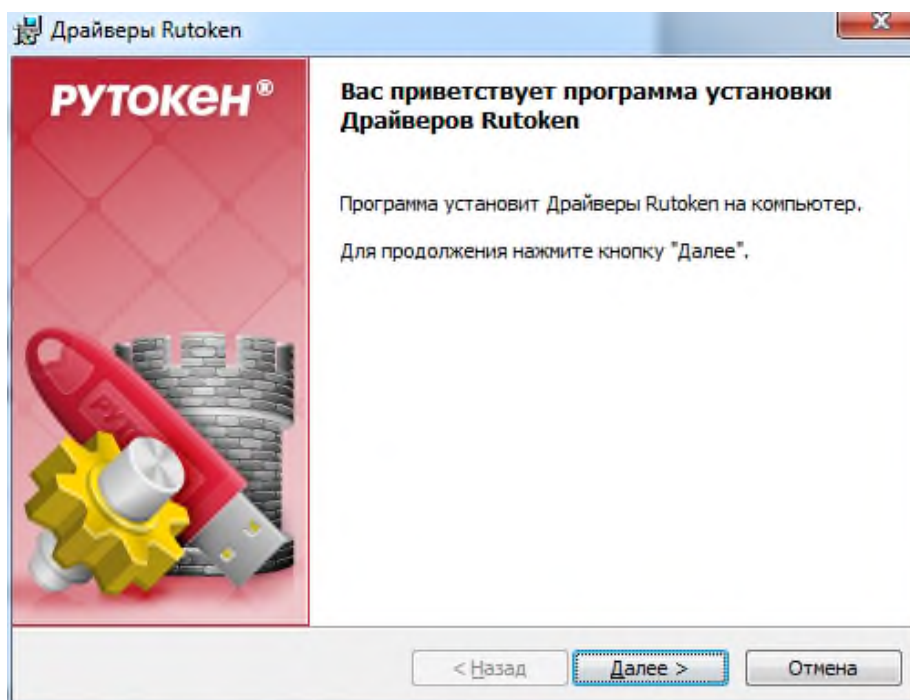
### 1.4.3. Установка драйвера используемого носителя ключевой информации сертификата пользователя

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

Если необходимый драйвер не установлен, необходимо:

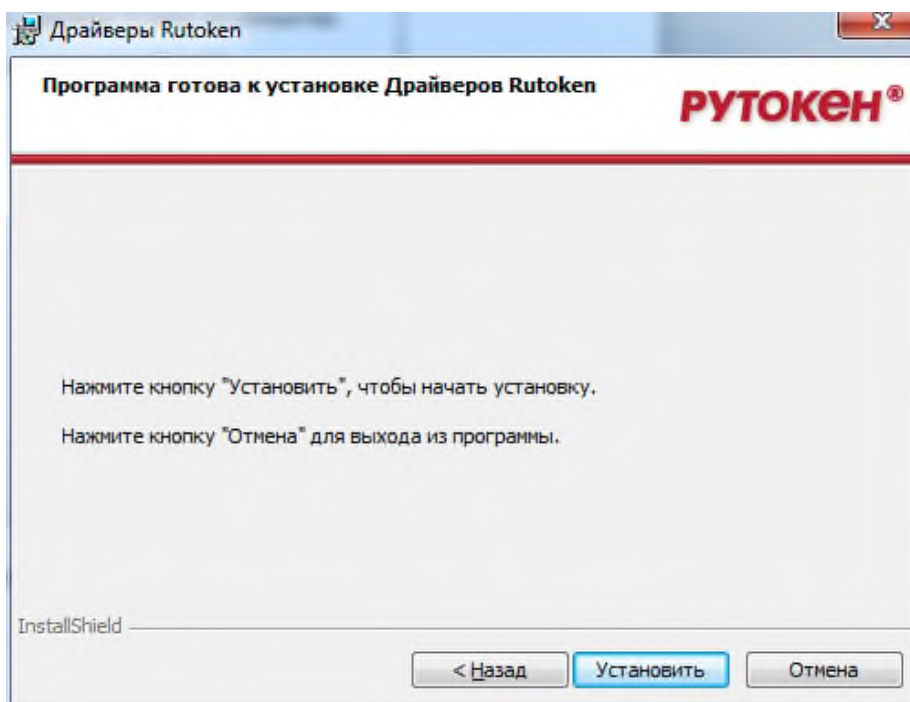
#### а) Драйвер носителя типа Rutoken

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 7).



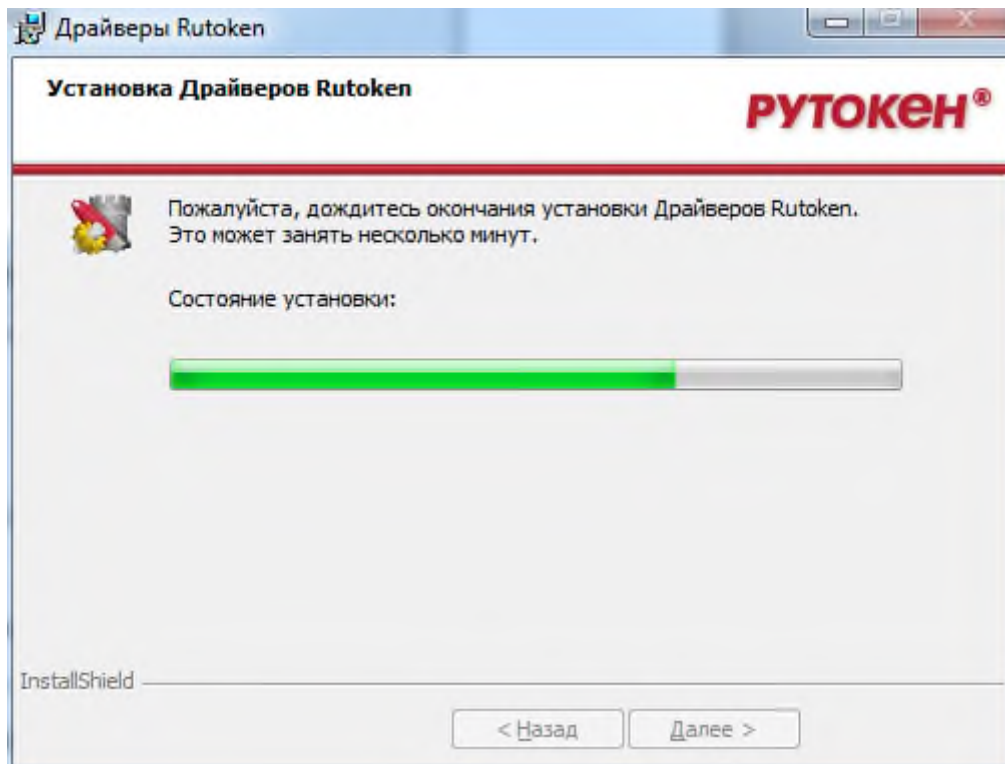
**Рисунок 7. Экранная форма приветствия установщика драйвера Rutoken**

2. Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов (Рисунок 8).



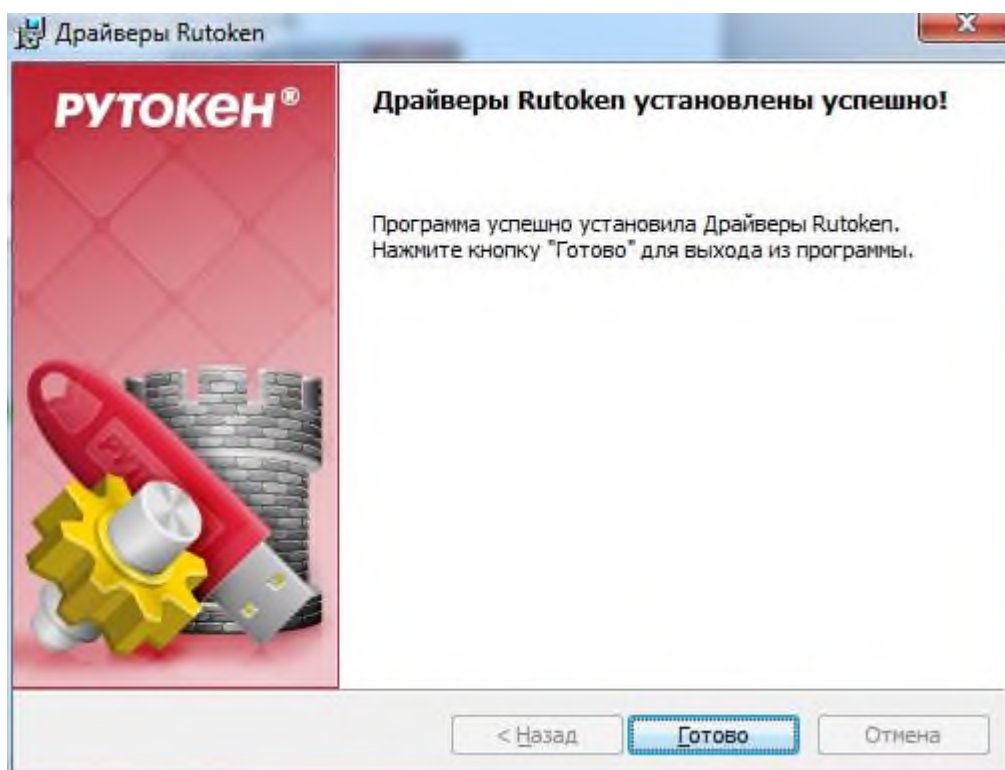
**Рисунок 8. Сообщение о готовности к выполнению установки драйверов**

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 9).



**Рисунок 9. Окно, информирующее о прогрессе установки драйверов Rutoken**

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 10).



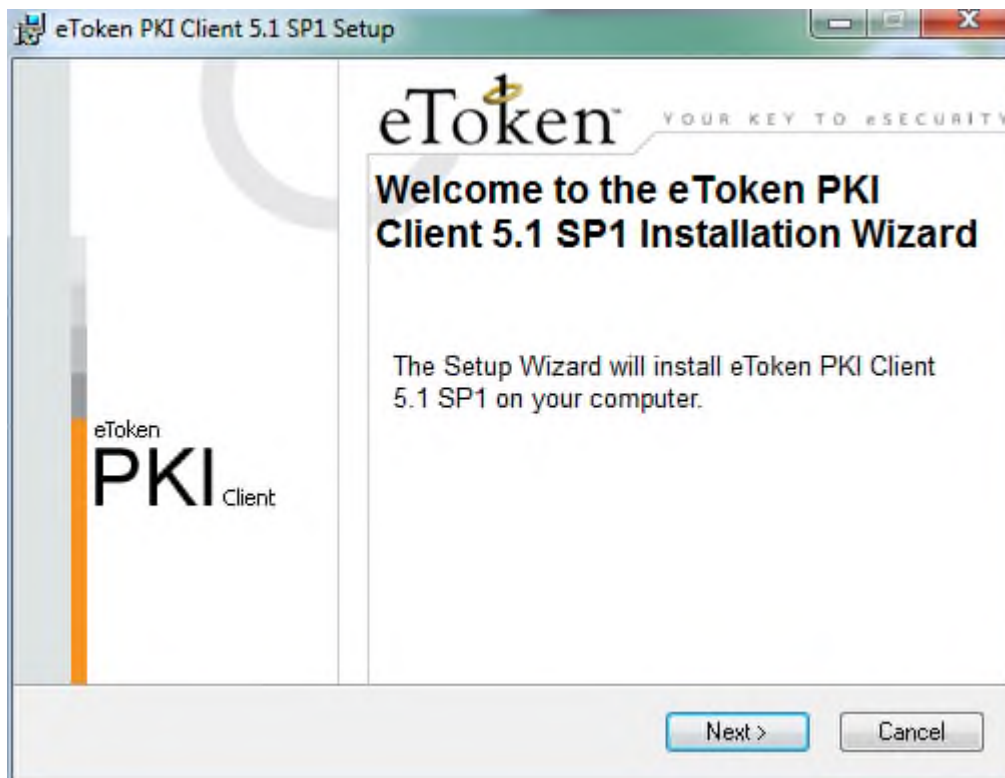
**Рисунок 10. Сообщение об успешной установке драйверов Rutoken.**

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 (JaCarta)**

1. Загрузите и запустите установочный файл, доступный на странице <https://www.aladdin-rd.ru/support/downloads/jacarta/>. Окно приветствия установщика драйвера eToken представлено на рисунке (Рисунок 11).



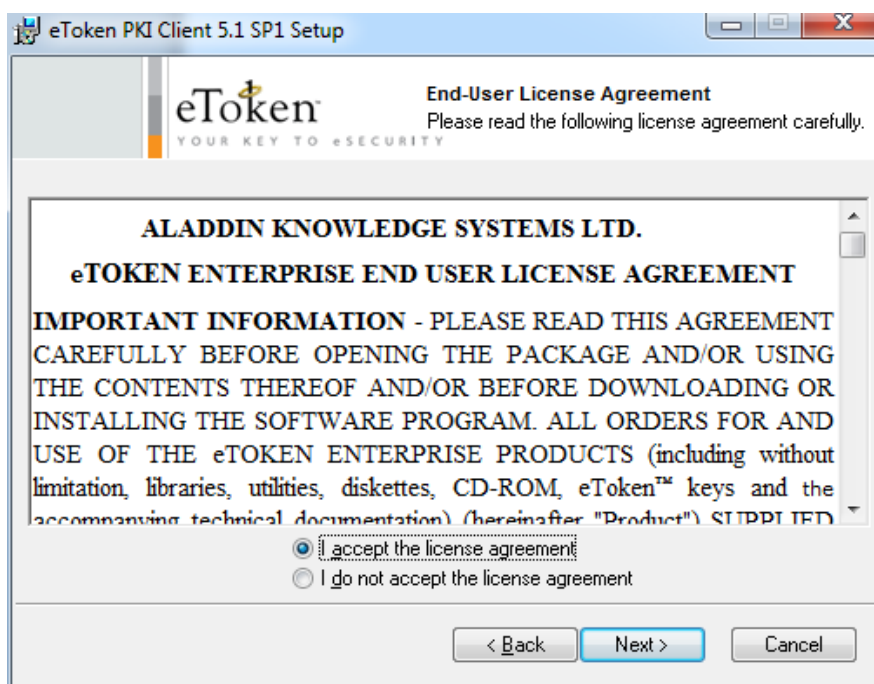
**Рисунок 11. Экранная форма приветствия установщика драйверов eToken**

2. Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (Рисунок 12).



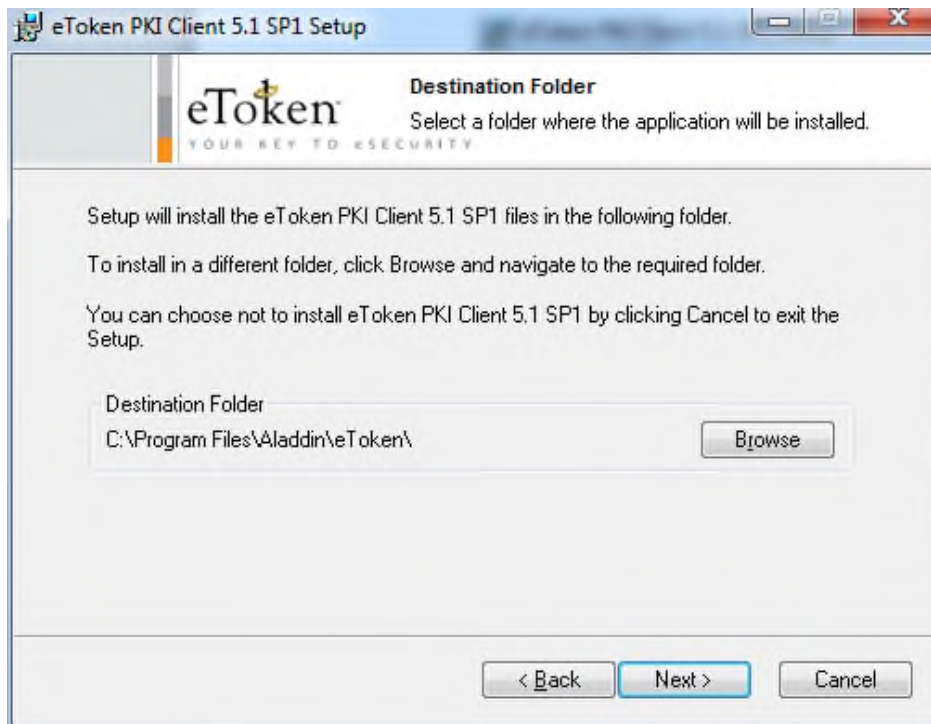
**Рисунок 12. Окно выбора языка программы, управляющей ключевыми носителями eToken**

3. В поле выберите язык «Русский» и нажмите «Next». На экране появится диалог лицензионного соглашения (Рисунок 13).



**Рисунок 13. Окно просмотра лицензионного соглашения**

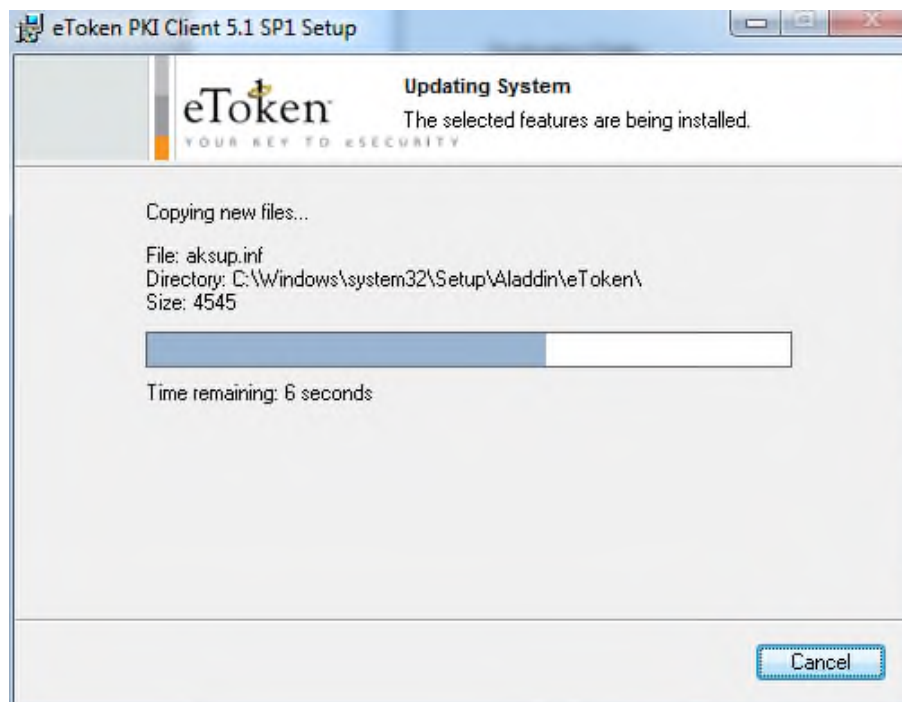
4. Выберите пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (Рисунок 14).



**Рисунок 14. Окно выбора пути для установки программы**

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

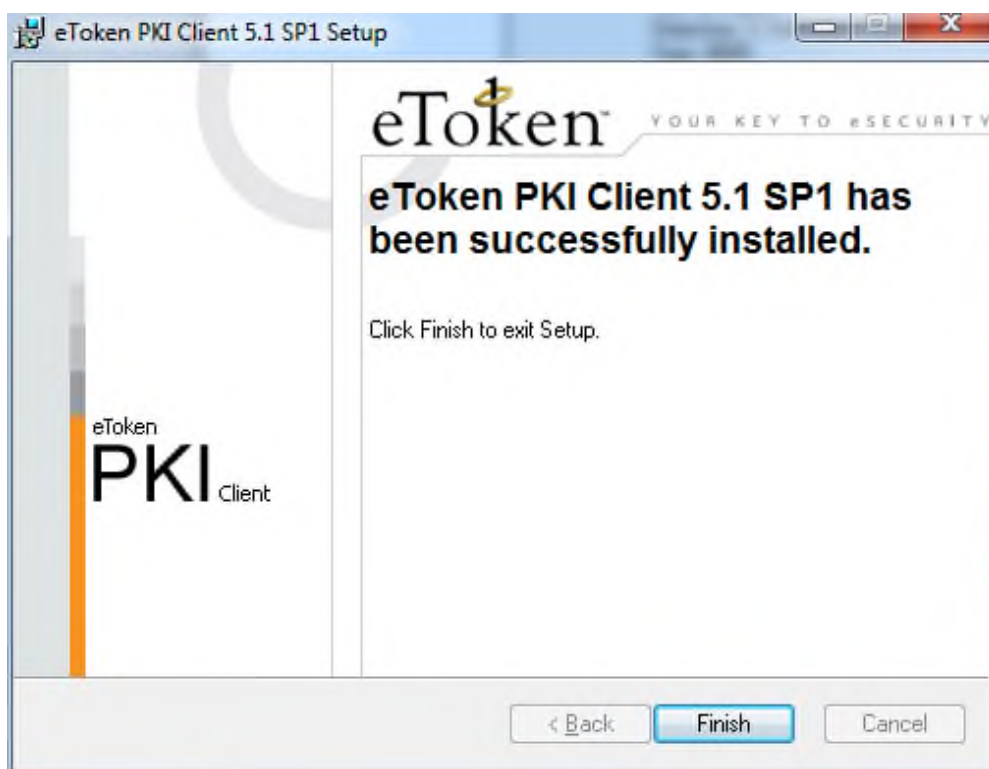
Начнется установка программы и драйверов. Диалог процесса установки представлено на рисунке (Рисунок 15).



**Рисунок 15. Прогресс установки драйверов eToken**

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 16).





**Рисунок 16. Сообщение об успешной установке драйверов Rutoken**

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

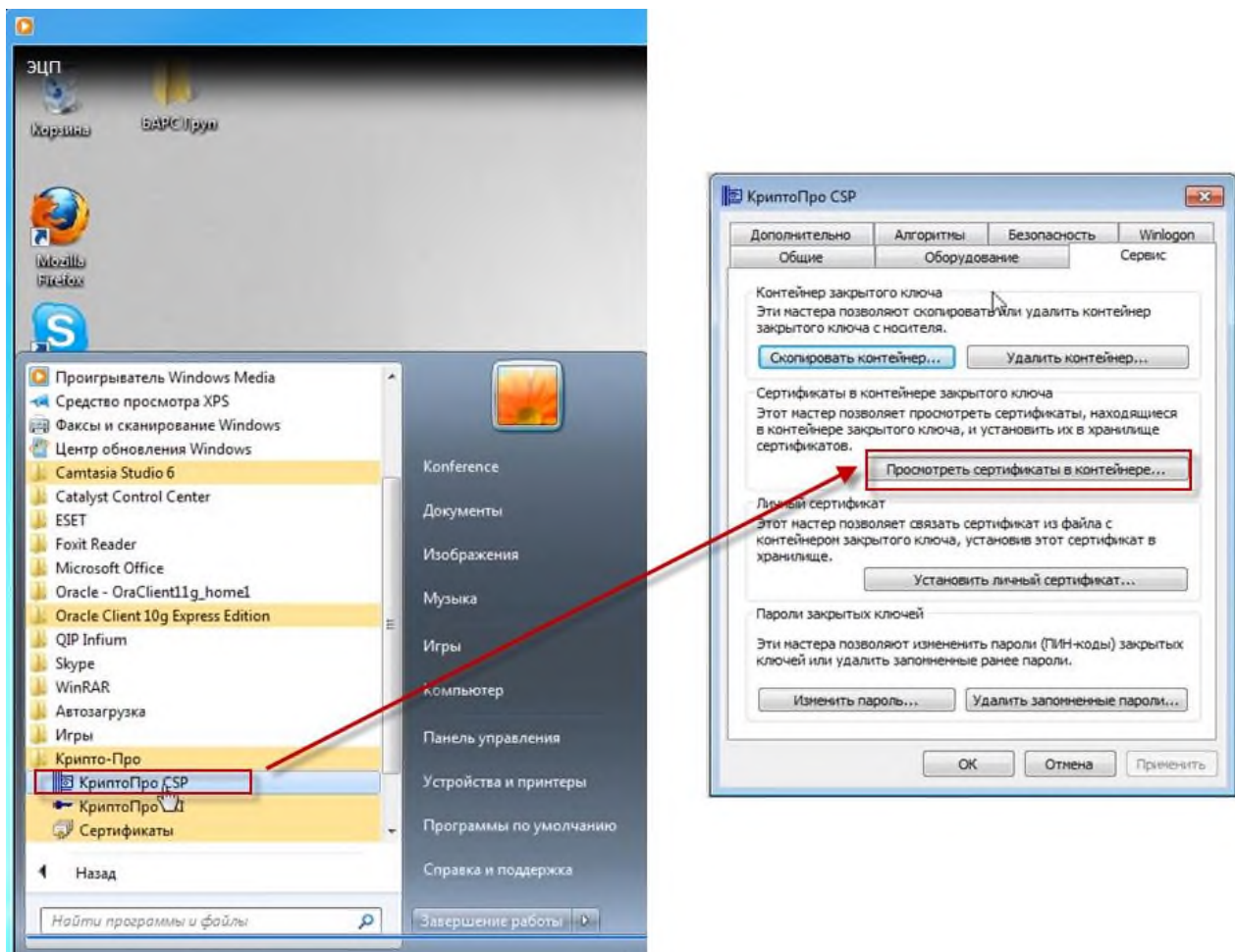
7. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места пользователя, ответить отрицательно или осуществить перезагрузку.

#### **1.4.4. 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:

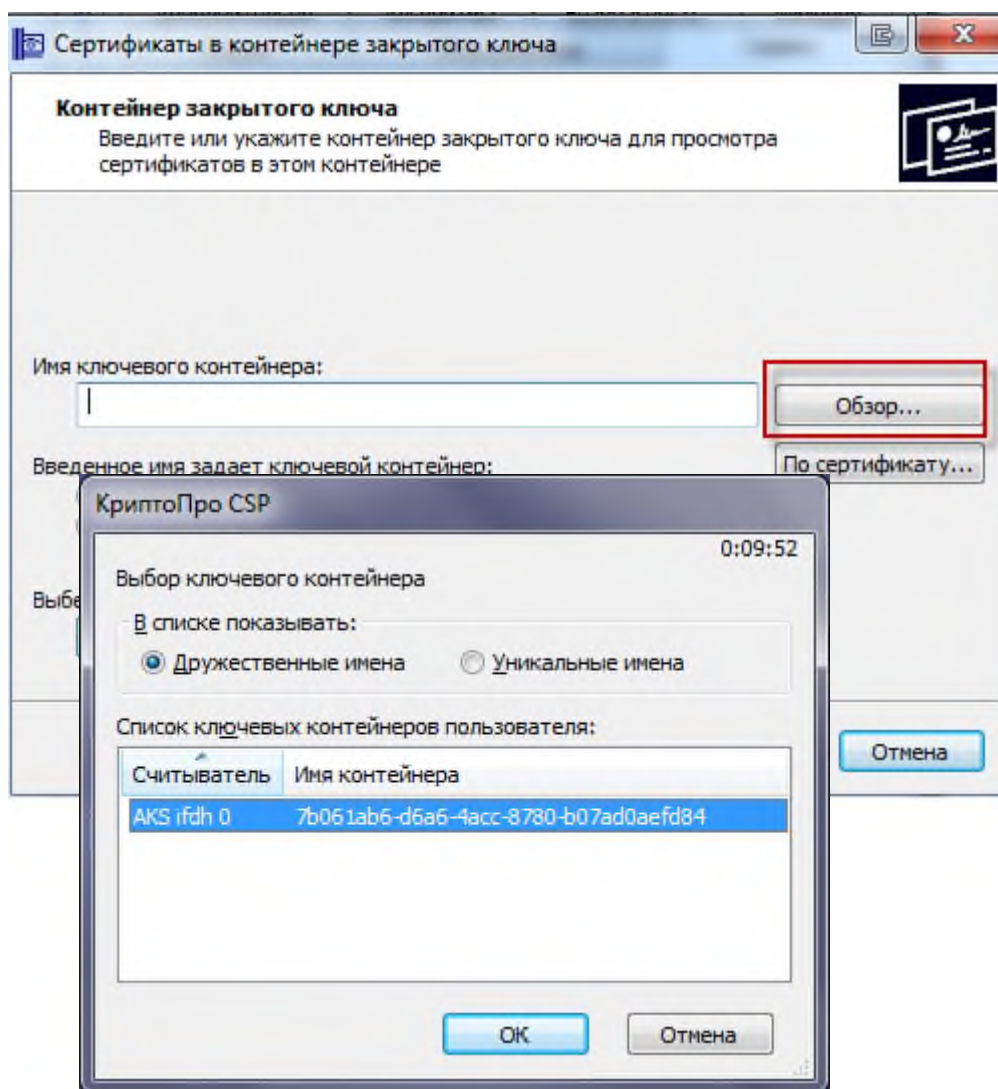
1. Запустите «КриптоПро CSP» (Пуск/Все программы/КриптоПро/КриптоПро CSP). В открывшемся окне на вкладке «Сервис» необходимо нажать на кнопку «Просмотреть сертификаты в контейнере» (Рисунок 17).



**Рисунок 17. Добавление ключа в хранилище**

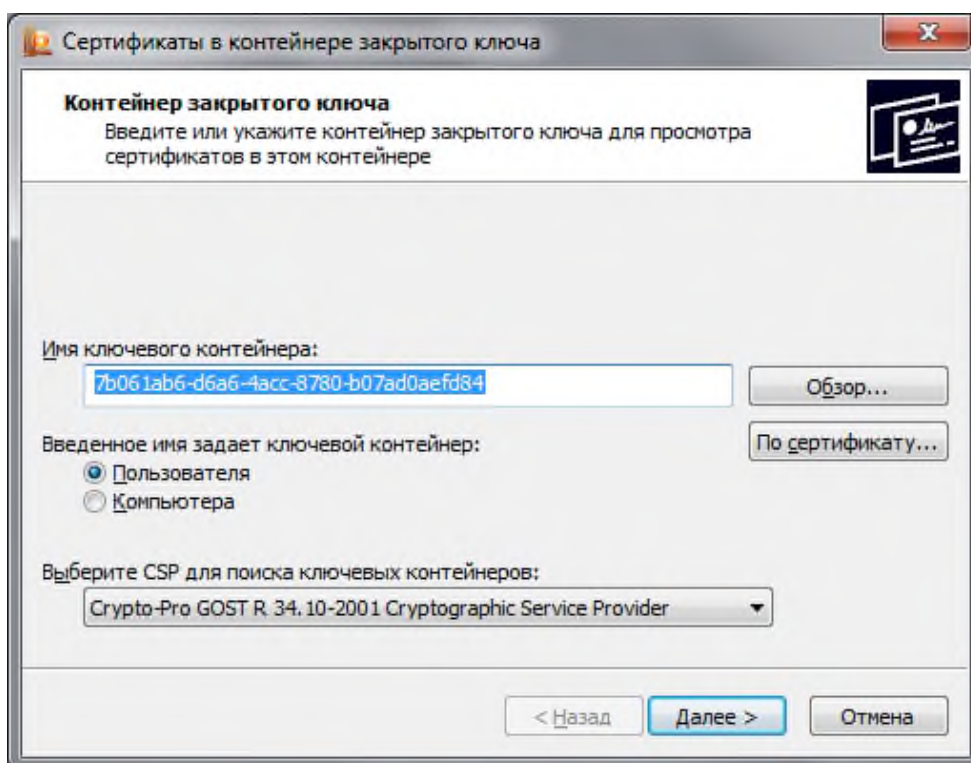
2. В открывшемся диалоговом окне «Сертификаты в контейнере закрытого ключа» нажмите на кнопку «Обзор» и выберите используемый ключ (предварительно установленный в USB-порт или дисковод ключ, предоставленный на носителе ruToken/eToken/JaCarta) (Рисунок 18). После этого нажмите на кнопку «ОК».





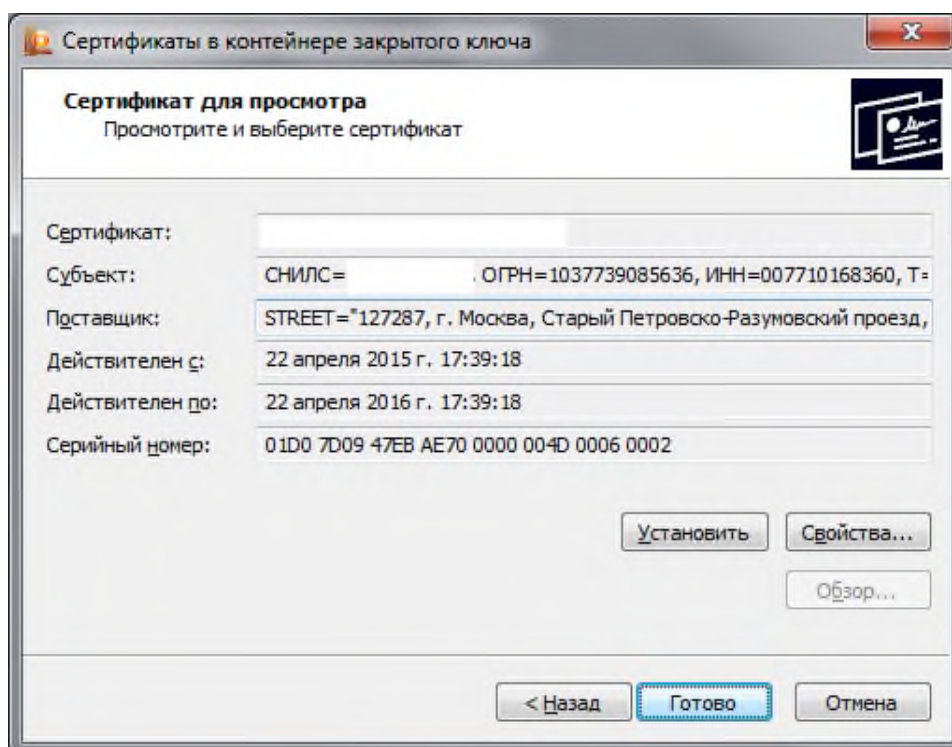
**Рисунок 18. Выбор ключевого контейнера**

3. Для завершения выбора контейнера закрытого ключа нажмите кнопку «Далее» (Рисунок 19)



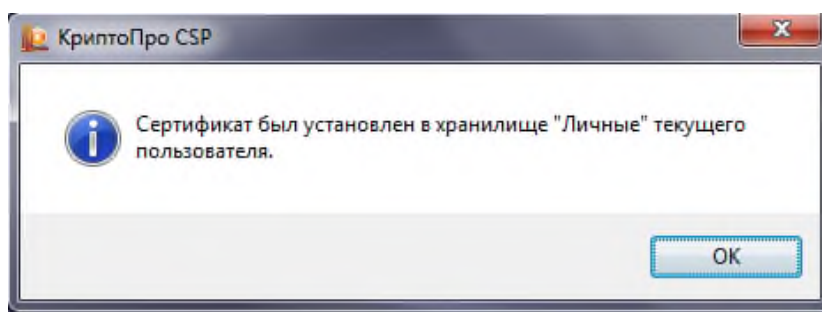
**Рисунок 19. Выбор контейнера закрытого ключа**

4. В открывшемся диалоговом окне нажмите на кнопку «Установить» (Рисунок 20):



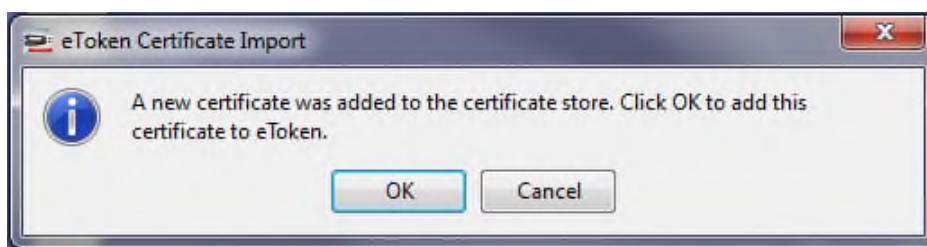
**Рисунок 20. Выбор сертификата**

5. После установки появится уведомление об успешной установке сертификата. Для подтверждения нажмите кнопку «ОК» (Рисунок 21).



**Рисунок 21. Уведомление об успешной установке сертификата**

Если в процессе выполнения действий появится сообщение «A new certificate was added to the certificate store» (Рисунок 22), необходимо нажать кнопку «Cancel».



**Рисунок 22. Сообщение драйвера eToken**

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

7. В открывшемся окне перейдите на вкладку «Путь сертификации» (Рисунок 23).

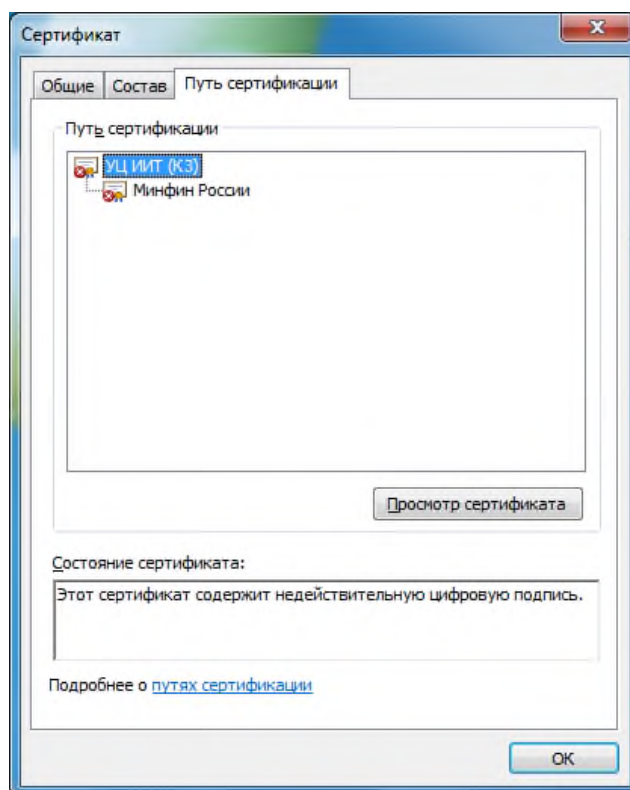
8. Проверьте, установлен ли сертификат верхнего уровня (сертификат доверенного корневого центра сертификации).

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

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

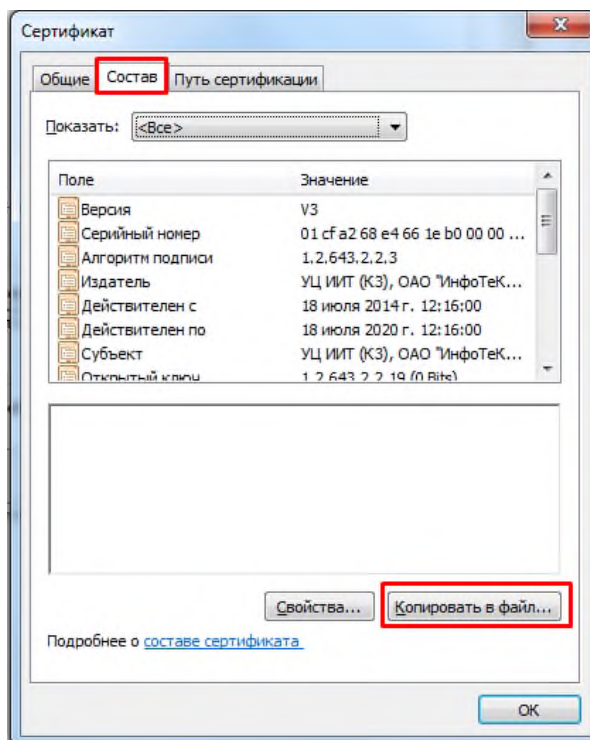
Если у первого в списке сертификата стоит знак 1, то нажатием левой кнопки мыши выберите данный сертификат.

Если у первого в списке сертификата стоит знак 2, переходите к шагу 22 раздела 1.3.3 данной инструкции.



**Рисунок 23. 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 24)



**Рисунок 24. 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».

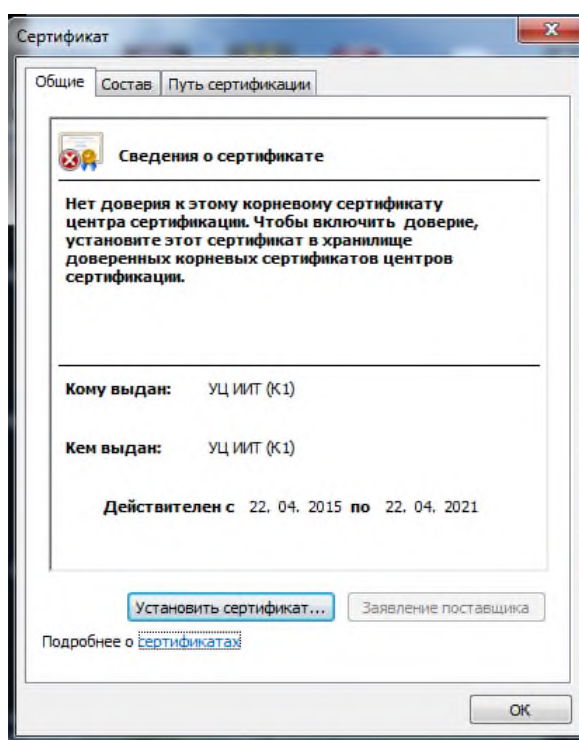
14. Убедитесь, что в окне «Имя экспортируемого файла» в поле «Имя файла» верно отобразился путь сохранения сертификата (например, C:\Users\0990\Desktop\Сертификат для ЭБ.cer). Нажмите кнопку «Далее».

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.cer».

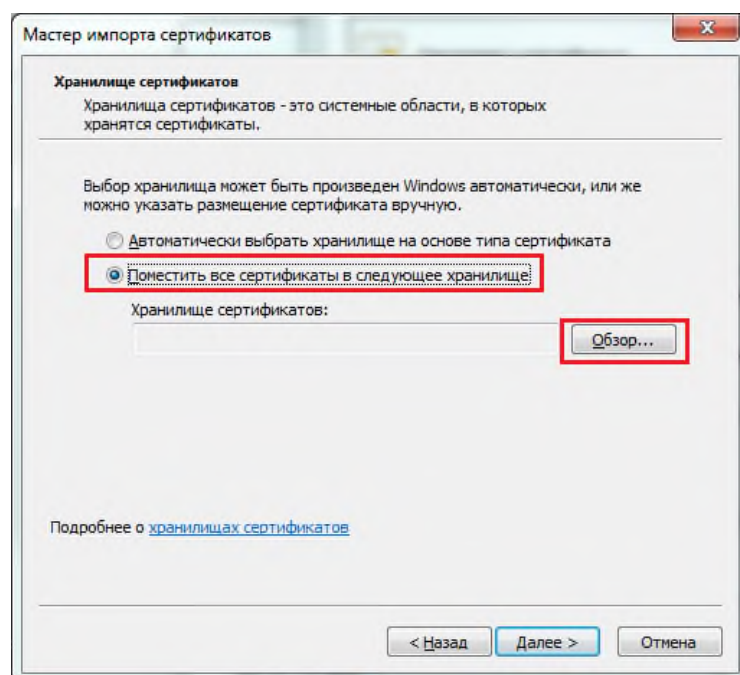
18. В появившемся окне нажмите на кнопку «Установить сертификат» (Рисунок 25). На экране отобразится мастер импорта сертификатов, где необходимо нажать кнопку «Далее».



**Рисунок 25. Установка корневого сертификата центра сертификации**

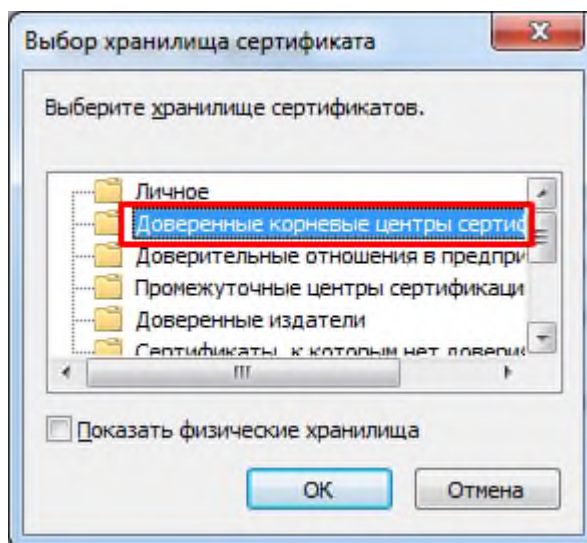
19. В окне «Хранилище сертификата» (Рисунок 26) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище». Нажать кнопку «Обзор...».





**Рисунок 26. Выбор хранилища сертификата**

20. В окне выбора хранилища сертификатов выберите контейнер «Доверенные корневые центры сертификации». Нажмите кнопку «Ок» (Рисунок 27).



**Рисунок 28. 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 20, 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 29).

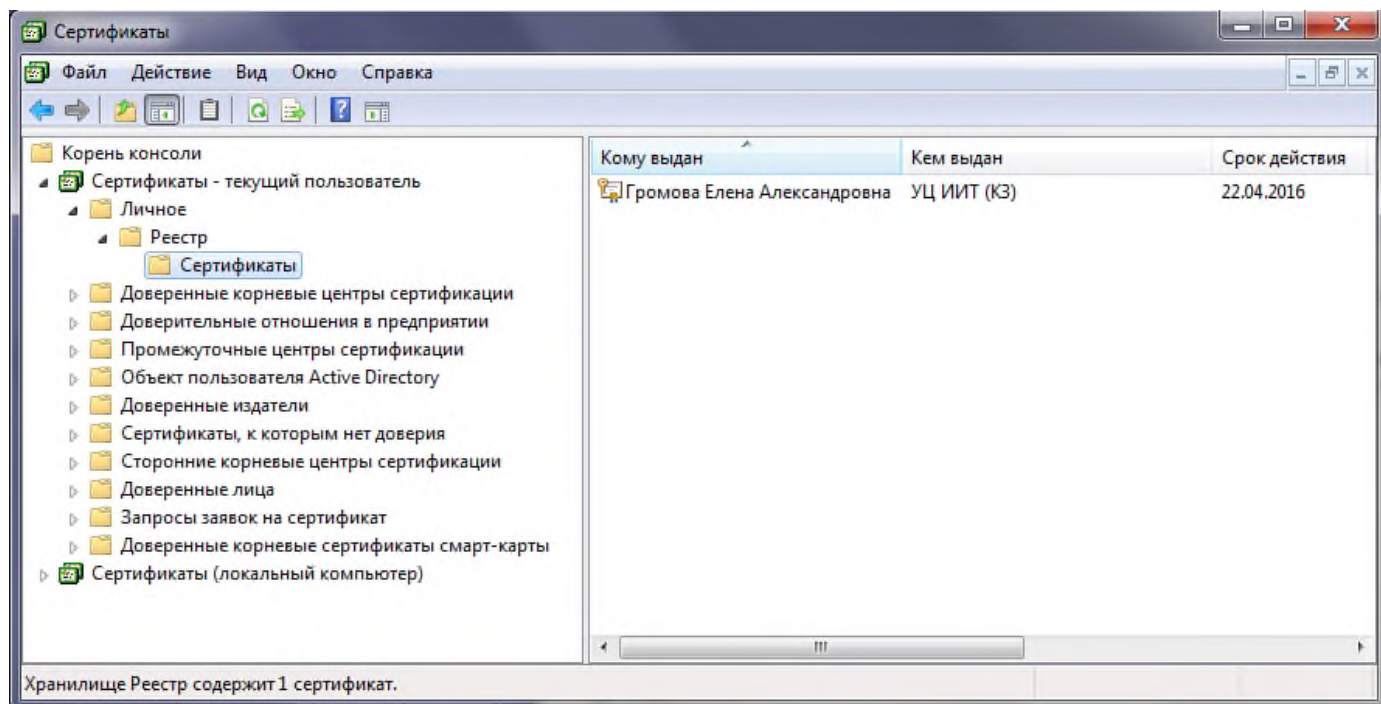


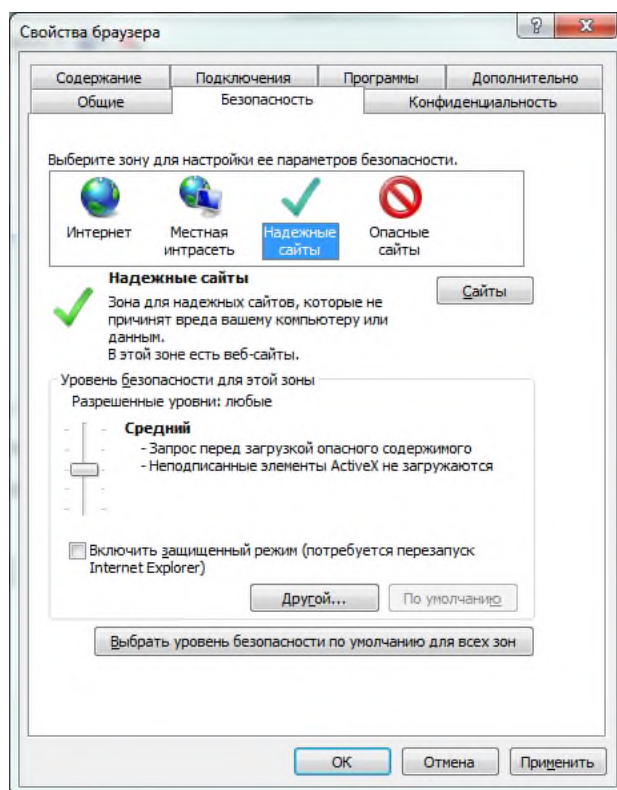
Рисунок 29. Утилита «Сертификаты»

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.

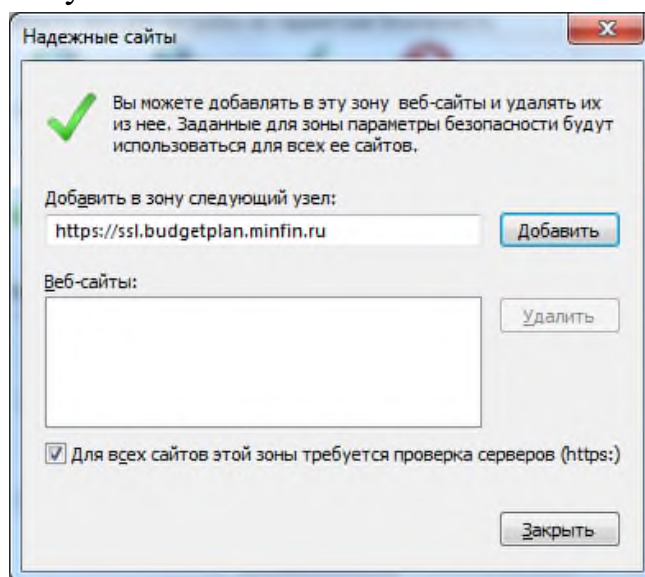
#### 1.4.5. Настройка Internet Explorer

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



**Рисунок 30. Диалог настройки безопасности браузера**

3. Выбрать зону для настройки «Надежные узлы» (Рисунок 30).
4. Нажать кнопку «Сайты».




**Рисунок 31. Диалог настройки доверенных узлов.**

5. В поле «Добавить в зону следующий узел» задать значение «https://ssl.budgetplan.minfin.ru/» и нажать кнопку «Добавить» (Рисунок 31).
6. В окне «Надежные сайты» нажать кнопку «Закреть».
7. В окне «Свойства браузера» нажать кнопку «ОК».



#### **1.4.6. Настройка «Яндекс.Браузер»**

1. Откройте настройки интернет-браузера посредством нажатия кнопки  → Настройки.
2. Перейдите в раздел Системные.
3. Убедитесь, что в разделе Сеть включена опция «Подключаться к сайтам, использующи шифрование по ГОСТ».

*В случае, отсутствия указанной опции установите актуальную версию интернет-браузер.*

#### **1.4.7. Установка корневого сертификата удостоверяющего центра Минфина России**

1. Скачайте файл корневого сертификат удостоверяющего центра Минфина России по ссылке <http://ssl.budgetplan.minfin.ru/CAMinfin.cer> .
2. Откройте загруженный файл caMinfin.cer.
3. Выполните действия, согласно шагам 18-21 раздела 1.4.4 данной инструкции.

## 2. ВХОД ПОДСИСТЕМУ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ И ПОДСИСТЕМУ УПРАВЛЕНИЯ НАЦИОНАЛЬНЫМИ ПРОЕКТАМИ СИСТЕМЫ

1. Для входа в Систему необходимо запустить интернет браузер «Internet Explorer» и в адресной строке ввести <http://budget.gov.ru/lk> (Рисунок 32).

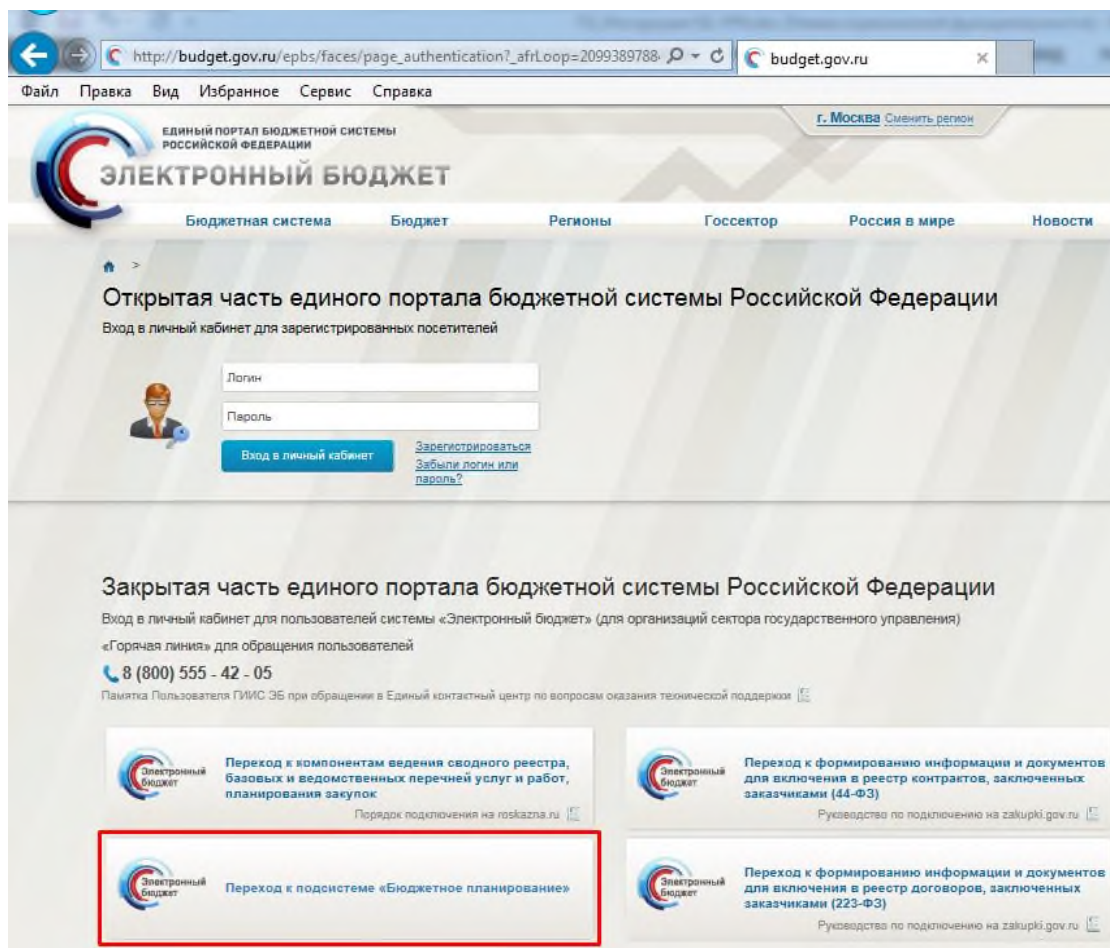


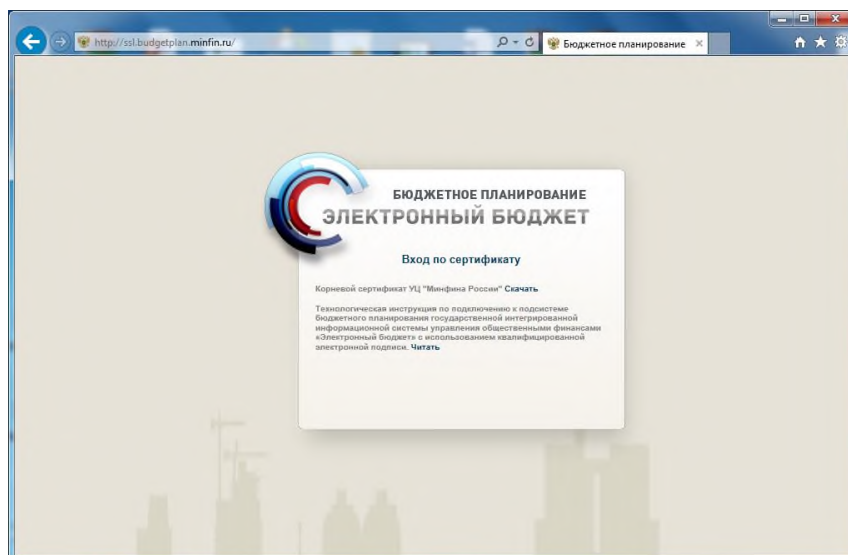
Рисунок 32. Единый портал бюджетной системы

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 <http://ssl.budgetplan.minfin.ru/> . Если перенаправление не произошло, введите указанную ссылку в адресную строку браузера.

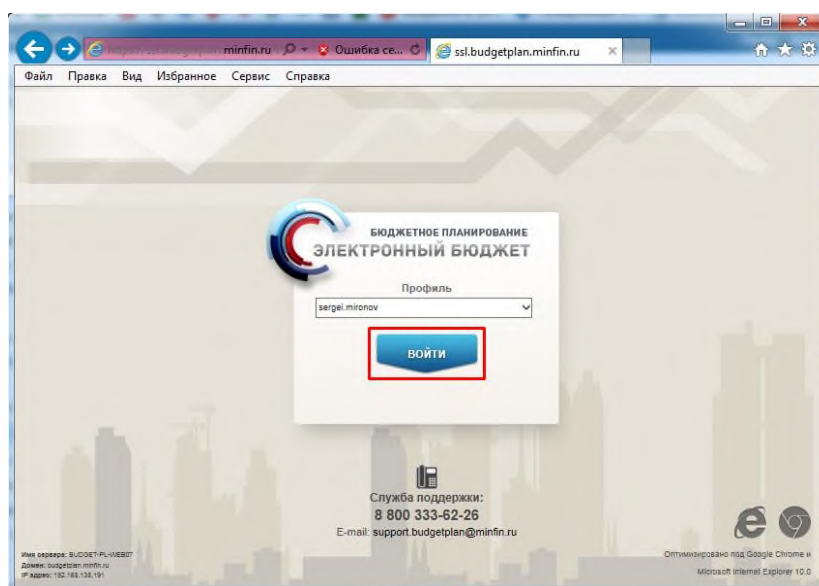
4. В появившемся окне, нажмите на кнопку «Вход по сертификату» (Рисунок 33).

5. После выбора метода аутентификации «Вход по сертификату», Система автоматически запросит сертификат и пин-код сертификата, затем произойдет поиск пользователя-владельца сертификата и открытие главного окна Системы.



**Рисунок 33. Окно выбора вида входа в систему**

Если различные пользователи используют для авторизации один сертификат (например, одно уполномоченное лицо имеет различные роли), то Система предложит выбрать конкретного пользователя (Рисунок 34). После выбора логина, необходимо нажать кнопку «Войти».



**Рисунок 34. Окно выбора логина пользователя**

6. При первом входе в систему, после успешной аутентификации уполномоченного лица участника системы «Электронный бюджет», отобразится форма Согласия на обработку персональных данных (Рисунок 35).

7. Заполните форму Согласия на обработку персональных данных актуальными сведениями.

Согласие может быть заполнено как вручную, так и посредством получения данных из сертификата посредством нажатия на кнопку «Заполнить ФИО из сертификата».

**Согласие на обработку персональных данных**

Я, Антонова Оксана Витальевна, проживающий по адресу (по месту регистрации)

Документ, удостоверяющий личность:

Наименование документа:

Серия паспорта:  Номер:  Дата выдачи:

название выдавшего органа:

В соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю свое согласие Министерству финансов Российской Федерации, Федеральному Казначейству и его территориальным органам на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, включающих фамилию, имя, отчество, должность, сведения о месте работы, адрес электронной почты, контактный (-е) телефон (-ы), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), в целях осуществления действий по подключению и работе в государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет». Предоставляю Министерству финансов Российской Федерации, Федеральному Казначейству и его территориальным органам право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

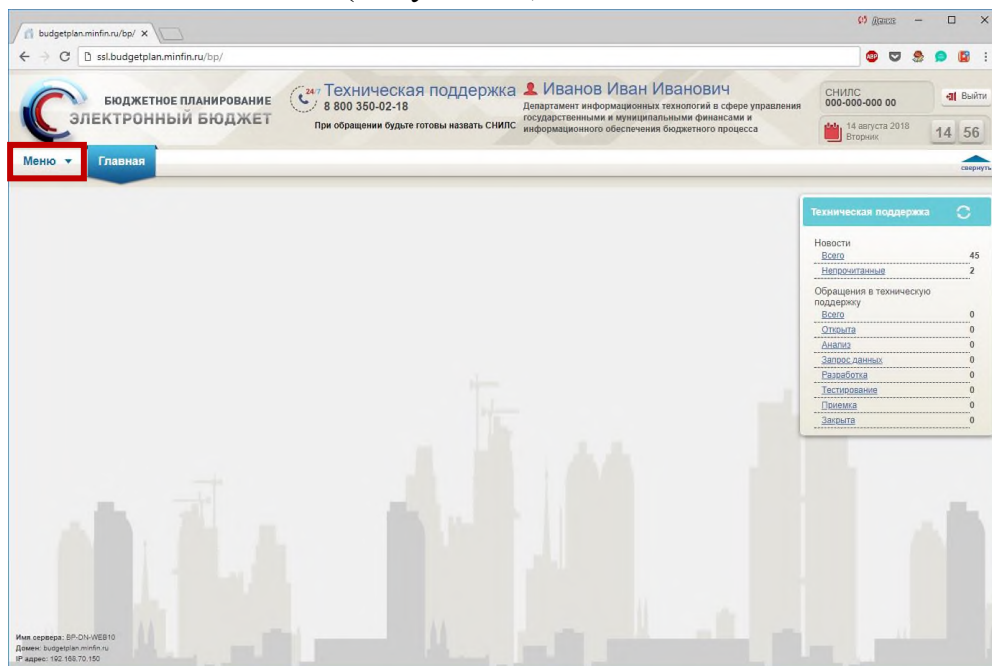
Срок действия настоящего согласия – период времени до истечения установленных нормативными актами сроков хранения соответствующей информации или документов, размещенных в государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет» с использованием моей электронной подписи.

Настоящее согласие на обработку персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных». В случае отзыва согласия на обработку моих персональных данных Министерство финансов Российской Федерации, Федеральное Казначейство и его территориальные органы вправе не прекращать их обработку до окончания срока действия настоящего согласия.

Информация обо мне, как субъекте обработки персональных данных в Соглашении на обработку персональных данных указана, верно

**Рисунок 35. Согласие на обработку персональных данных**

8. После заполнения формы нажмите кнопку «Подписать».
9. После завершения подписи Соглашения на обработку персональных данных отобразится рабочее окно Системы (Рисунок 36).



**Рисунок 36. Рабочее окно Системы**



### 3. ПРОБЛЕМЫ ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ И ИХ УСТРАНЕНИЕ

#### 3.1. Проблема с сертификатом безопасности

Если между шагами 4 и 5 раздела 2 данной инструкции появляется сообщение «Возникла проблема с сертификатом безопасности этого веб-сайта» (Рисунок 37), необходимо выполнить действия согласно разделу 1.4.7. данной инструкции.

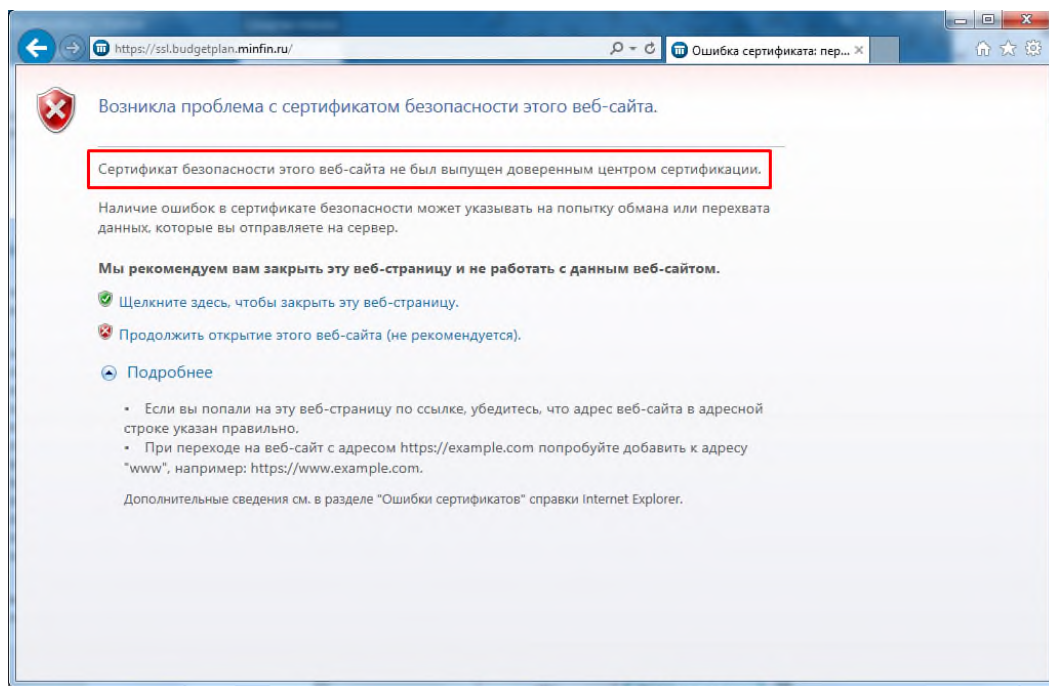
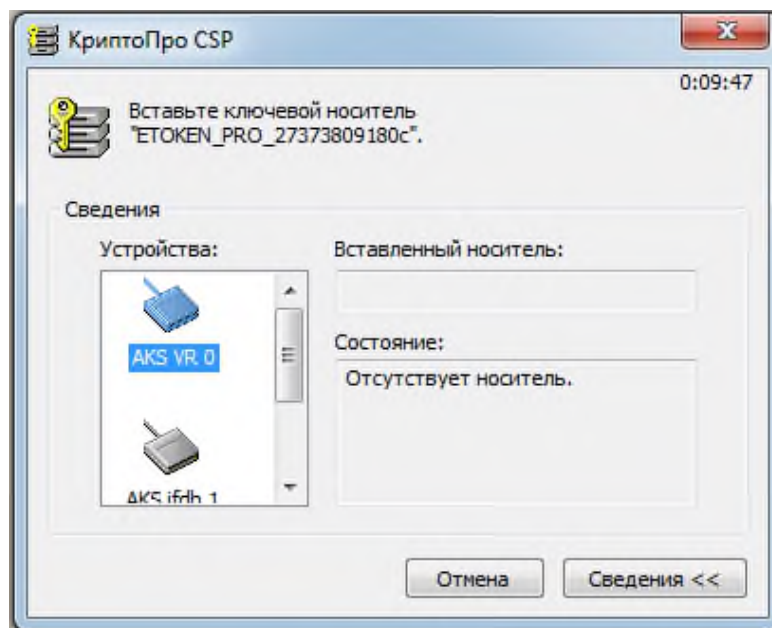


Рисунок 37. Проблема с сертификатом безопасности

#### 3.2. Вставьте ключевой носитель

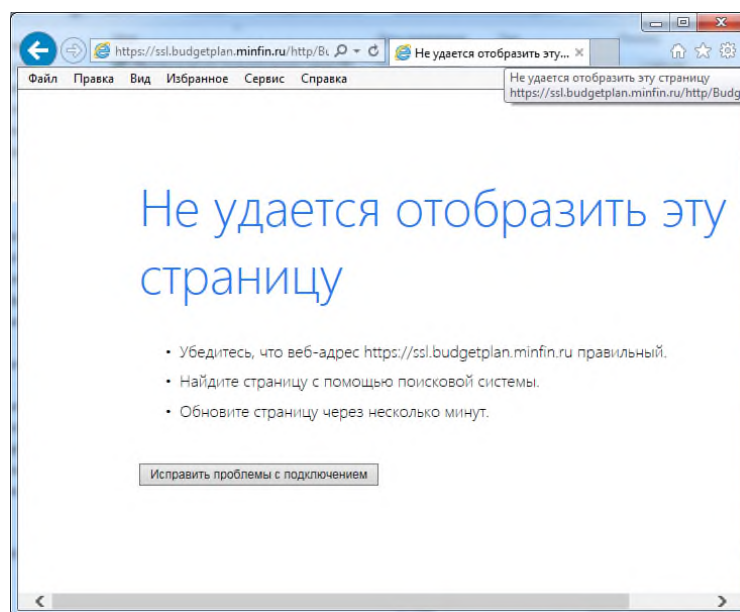
Если между шагами 4 и 5 раздела 2 данной инструкции появляется сообщение «КриптоПРО CSP» «Вставьте ключевой носитель» (Рисунок 38), необходимо:

1. Установить сертификат, предоставленный на носителе ruToken/eToken (JaCarta)/flash-накопителе/дискете.
2. Перезапустить интернет-браузер.
3. Повторите шаги раздела 2 данной инструкции.



**Рисунок 38. Вставьте ключевой носитель**

### **3.3. Не удается отобразить эту страницу**



**Рисунок 39. Не удается отобразить эту страницу**

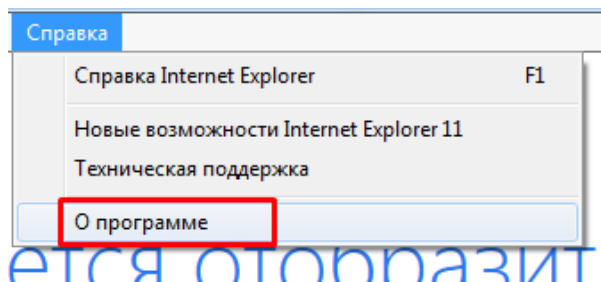
Если появляется сообщение об ошибке «Не удастся отобразить эту страницу» (Рисунок 39), необходимо:

1. Убедиться, что включена возможность подключения к сайтам, использующим шифрование по ГОСТ в соответствии с пунктом 1.4.6 (при использовании «Яндекс.Браузера») или проверить версию браузера Internet Explorer (версия должна быть не ниже Internet Explorer 10) при необходимости обновить интернет-браузер.

Для проверки версии:

откройте интернет-браузер Internet Explorer;

в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 40) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.



**Рисунок 40. О программе**

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установить (см. раздел 1.4.1. данной инструкции).

3. Проверить в браузере ссылку, по которой осуществляется вход.

Вход в систему возможен только по ссылке <http://ssl.budgetplan.minfin.ru> или <https://ssl.budgetplan.minfin.ru> без добавления дополнительных директорий к адресу сайта (например, <https://ssl.budgetplan.minfin.ru/http/budgetplan>).

4. Проверить наличие других криптопровайдеров (например, «VipNet CSP», «Lissi CSP», «Валидата CSP» и др/) кроме «КриптоПро CSP». При обнаружении осуществить деинсталляцию всех криптопровайдеров, в том числе «КриптоПро CSP», и провести очистку следов установки продуктов «КриптоПро CSP», путем запуска с правами администратора утилиты `cspclean.exe` (<http://www.cryptopro.ru/sites/default/files/public/cspclean.exe>).

После очистки необходимо произвести повторную установку и настройку КриптоПро CSP согласно разделу 1.4.1 данной инструкции, далее повторно установить иные криптопровайдеры с соблюдением последовательности приведенной в п. 3.6 данной инструкции.

5. Временно отключить антивирусные средства на автоматизированном рабочем месте пользователя Системы, в особенности, если на автоматизированном рабочем месте пользователя Системы установлены бесплатные антивирусные средства. После отключения антивирусных средств проверить возможность входа в Систему, согласно разделу 2 данной инструкции.

### **3.4. Окно ввода логина и пароля**

В случае возникновения окна ввода логина и пароля между шагами 4 и 5 раздела 2 данной инструкции (Рисунок 41), необходимо:

1. Убедиться в том, что уполномоченному лицу присвоен логин (цифробуквенная последовательность в формате `000_AAAA*.В.С`, высылается на адрес уполномоченного лица после утверждения заявки в Минфине России).

В случае, если данные об учетной записи отсутствуют, за разъяснением порядка регистрации пользователей обращайтесь в службу поддержки Системы по телефону 8 800 350-02-18.

2. Убедиться в том, что в автоматизированном рабочем месте установлен сертификат лица, которому присвоен логин.

3. Убедиться в том, что СНИЛС владельца сертификата (указан в поле субъект сертификата) соответствует значению СНИЛС в Системе.

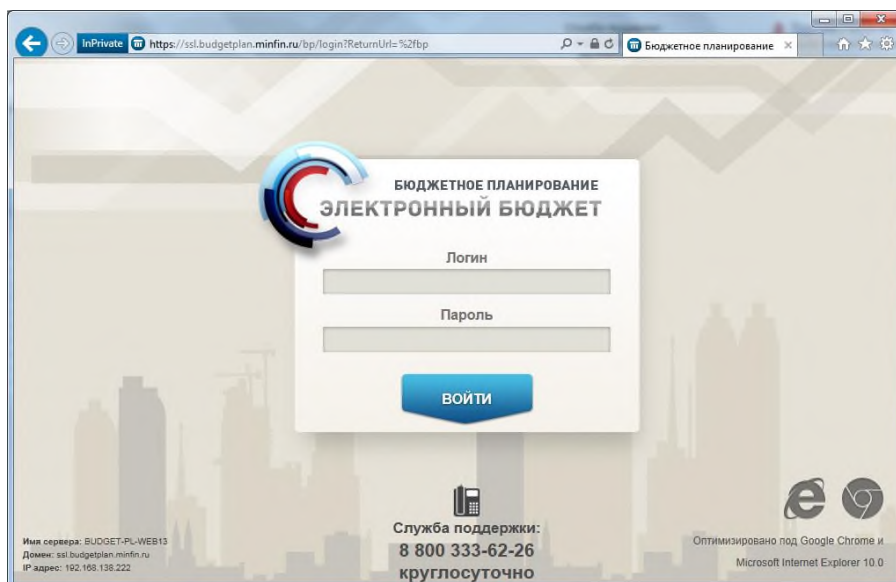


Рисунок 41. Окно ввода логина и пароля

### 3.5. Не удается отобразить эту страницу. Включите протоколы TLS

Если появляется сообщение об ошибке «Не удастся отобразить эту страницу» (Рисунок 42), необходимо:

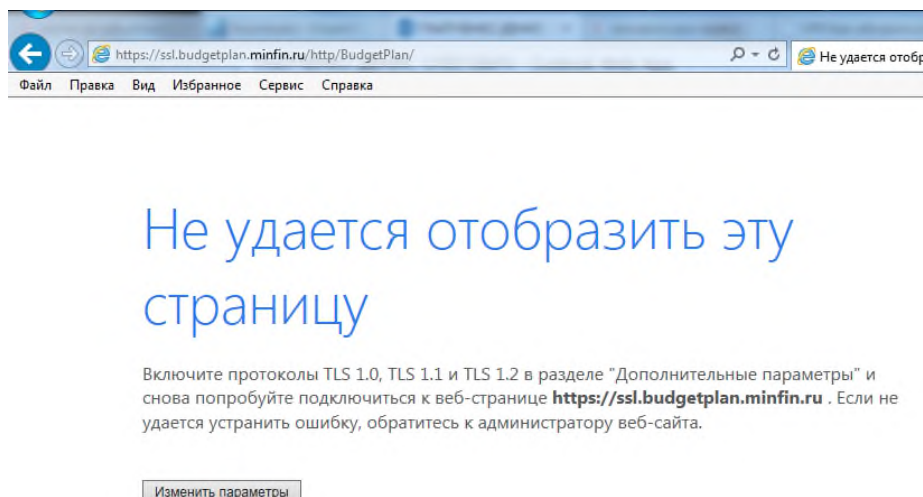


Рисунок 42. Не удастся отобразить эту страницу. Включите протоколы TLS

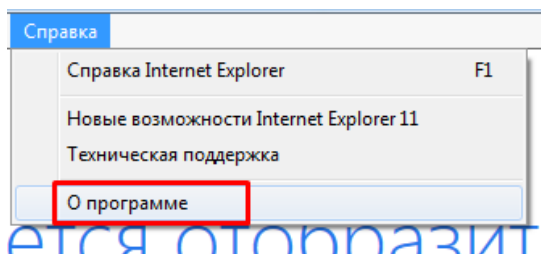
1. Убедиться, что включена возможность подключения к сайтам, использующим шифрование по ГОСТ в соответствии с пунктом 1.4.6 (при использовании «Яндекс.Браузера») или проверить версию браузера Internet Explorer



(версия должна быть не ниже Internet Explorer 10) при необходимости обновить интернет-браузер.

Для проверки версии интернет-браузера Internet Explorer:  
откройте браузер Internet Explorer;

в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 40) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.



**Рисунок 43. О программе**

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установите (см. раздел 1.4.1. данной инструкции).

3. Проверить наличие других криптопровайдеров (например, «VipNet CSP», «Lissi CSP», «Валидата CSP» и др/) кроме «КриптоПРО CSP». При обнаружении осуществить деинсталляцию всех криптопровайдеров, в том числе «КриптоПРО CSP», и провести очистку следов установки продуктов КриптоПро, путем запуска с правами администратора утилиты cspclean.exe (<http://www.cryptopro.ru/sites/default/files/public/cspclean.exe>).

После очистки необходимо произвести повторную установку и настройку «КриптоПРО CSP» согласно разделу 1.4.1 данной инструкции, далее повторно установить иные криптопровайдеры с соблюдением последовательности приведенной в п. 3.6 данной инструкции.

### **3.6. Устранение ошибок, возникающих при совместном использовании «КриптоПро CSP» совместно с «Континент TLS-клиент»**

Криптопровайдеры («КриптоПРО CSP», «Валидата CSP», «VipNet CSP», «Lissi CSP») и программное обеспечение «Jinn-Client» необходимо устанавливать до установки Континент TLS-клиент, соблюдая следующую последовательность установки:

- криптопровайдер;
- программное обеспечение «Jinn-Client»;
- «Континент TLS-клиент».

При нарушении этого условия в процессе работы с Системой могут возникнуть ошибки, описанные в разделах 3.3 и 3.5 данной инструкции.

Для исправления проблемы в данном случае необходимо:

1. Удалить все вышеперечисленные программные продукты.
2. После каждого удаления программного продукта выполнить перезагрузку рабочего места, если она требуется.
3. Установить программные продукты заново в соответствии с описанным порядком.

### **3.7. 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 1.4.4. инструкции сохранить сертификат корневого центра сертификации;

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

отправить архив на адрес электронной почты [support-tls@minfin.ru](mailto:support-tls@minfin.ru) с указанием наименования организации, ИНН организации, наименования вышестоящего федерального органа исполнительной власти (при наличии), СНИЛС пользователя.

При возникновении вопросов, связанных с функционированием Системы необходимо обращаться по телефону 8 800 350-02-18 или оставить обращение в электронной форме с использованием раздела Системы «Техническая поддержка» доступного с использованием в меню Системы.