Код Безопасности

Программно-аппаратный комплекс
квалифицированной электронной подписи

"Jinn". Версия 1.0

Руководство пользователя

RU.88338853.501430.008 92

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данное руководство предназначено для пользователей изделия "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn". Версия 1.0" RU.88338853.501430.008 (далее — ПАК "Jinn", изделие, комплекс). В нем содержатся сведения, необходимые для работы с ПАК "Jinn".

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения

В корпоративных, территориально распределенных информационных системах могут циркулировать электронные документы, требующие заверения электронной подписью. Существует и признается актуальной атака "человек посередине". Этим человеком может быть физическое лицо, непосредственно взаимодействующее с компьютером ответственного за работу с документом лица, или удаленный злоумышленник, который действует посредством программной атаки (всевозможные вирусы, трояны, черви, руткиты и т. д.) на компьютер ответственного лица из глобальной или локальной сети. Если с первым типом злоумышленника (физическое лицо) можно бороться только организационными мерами, то со вторым необходимо бороться программными или программно-аппаратными средствами. Для защиты именно от второго типа злоумышленника предлагается решение ПАК "Jinn".

Назначение и основные функции

ПАК "Jinn" предназначен для формирования электронной подписи (ЭП) электронного документа, расположенного в ОЗУ компьютера в виде XML-документа, текстового или бинарного файла. Формирование ЭП осуществляется в соответствии с положениями ст. 12 Федерального закона РФ "Об электронной подписи" от 06.04.11 № 63-ФЗ.

ПАК "Jinn" реализует следующие основные функции:

- визуализация электронного документа при отображении подписываемого или проверяемого электронного документа;
- формирование электронной подписи в соответствии с ГОСТ Р 34.10–2001, ГОСТ Р 34.11–94, ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012;
- генерация ключей электронной подписи и формирование запросов на создание сертификатов.

Для проверки правильности работы алгоритма выработки ЭП в комплексе реализована вспомогательная функция контрольного тестирования. Данная функция не используется в качестве целевой функции проверки ЭП.

ПАК "Jinn" можно эксплуатировать совместно со следующими программными продуктами (для файлов с расширениями .txt, .odt, .xml, .pdf) без проведения тематических исследований и/или оценки влияния:

- Adobe Acrobat Reader (от версии 11.0 и выше);
- MS Word 2007, Word 2010, Word 2013.

Назначение электронной подписи

Электронная подпись документа представляет собой данные в электронной форме, присоединяемые к подписываемому электронному документу. Она получается в результате криптографического преобразования информации с использованием ключа подписи.

Электронная подпись позволяет определить лицо, подписавшее электронный документ, а также установить наличие искажений информации в документе. Использование ЭП повышает уровень защищенности документооборота корпоративных информационных систем.

Правовые условия применения ЭП в электронных документах определяются положениями Федерального закона РФ "Об электронной подписи" от 06.04.11 №63-ФЗ. Согласно закону в защищенном документообороте могут использоваться три вида ЭП: простая, неквалифицированная и квалифицированная.

Алгоритмы и процедуры создания ЭП задаются государственными стандартами: формирование и проверка ЭП — ГОСТ Р 34.10–2012, ГОСТ Р 34.10–2001, вычисление хэш-функции — ГОСТ Р 34.11–2012, ГОСТ Р 34.11–94.

Назначение ключевых носителей

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения ключевой информации — ключа подписи и сертификата ключа. При подписании документа пользователь предъявляет ключевой носитель, ключевая информация считывается с носителя и с ее помощью создается ЭП пользователя.

Ключ подписи хранится в памяти ключевого носителя в криптографическом контейнере. Криптографический контейнер представляет собой специальным образом организованную папку, содержащую файлы с ключевым материалом. Для предотвращения несанкционированного использования ключа подписи посторонними лицами криптографический контейнер защищают паролем. Ключевой носитель может содержать несколько контейнеров с различными ключами.

Ключ подписи должен однозначно соответствовать сертификату ключа. Для создания ЭП в ПАК "Jinn" предусмотрены два варианта хранения сертификата: на ключевом носителе и в личном хранилище сертификатов Windows.

В качестве ключевых носителей в комплексе могут использоваться аппаратные носители двух типов: USB-флеш-накопители, USB-ключи (Рутокен, eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash) и смарт-карты (eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ).

Для создания ЭП в доверенной среде пользователю комплекса помимо ключевых носителей потребуется идентификатор для входа в ПАК "Соболь" (iButton/USB-ключ (eToken PRO, eToken PRO (Java), iKey 2032, Рутокен, Рутокен RF)/смарт-карта eToken PRO) или загрузочный USB-флеш-накопитель.

Глава 2
Настройка ПАК "Jinn"

Для использования ПАК "Jinn" необходимо получить сертификат пользователя.

Сертификаты открытых ключей

Сертификат — это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

ПАК "Jinn" может работать с сертификатами в формате PKCS 10 (обычно с расширением *.p10b). Могут содержать несколько сертификатов, например, цепочку подтверждающих друг друга сертификатов. В таком формате хранятся сертификаты корневого центра сертификации.

Сертификаты в файлах с расширением *.p10b соответствуют стандарту X.509v3 Международного телекоммуникационного союза (ITU-T).

Система автоматически отслеживает статус сертификата — действителен или недействителен. Недействительным сертификат может быть признан по следующим причинам:

- срок действия сертификата не наступил;
- срок действия сертификата истек;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Управление сертификатами

Для настройки ПАК "Jinn" выполните следующие действия:

- создайте файл запроса на получение сертификата пользователя (см. ниже);
- передайте администратору созданный файл запроса;
- на основании полученного от пользователя запроса администратор создает сертификат и передает его пользователю на закрытом ключевом носителе.

Для настройки потребуется носитель, содержащий ключевую информацию (ключевой носитель). Ключевым носителем может являться присвоенный пользователю персональный идентификатор (тот же, который используется для идентификации, или другой), дискета, флеш- карта или USB-флеш-накопитель.

Создание запроса на сертификат

ПАК "Jinn" позволяет создать запрос на издание сертификата пользователя по стандарту PKCS#10.

Запрос на получение сертификата создается пользователем ПАК "Jinn" по мере необходимости. Одновременно с запросом будет создан закрытый ключ сертификата пользователя, при этом пользователь самостоятельно назначает пароль доступа к ключевому контейнеру. Созданный запрос на получение сертификата пользователь передает администратору безопасности, а закрытый ключ хранит у себя.

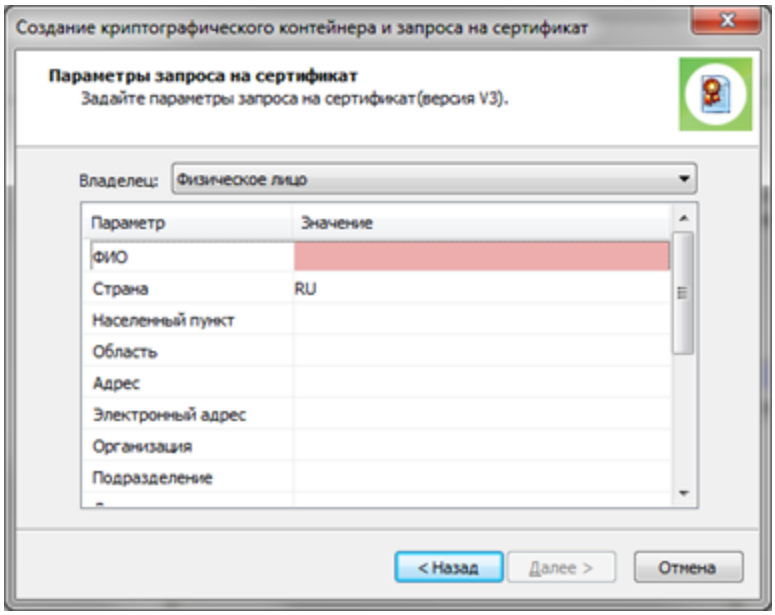
Для создания запроса:

1. Нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы|Код Безопасности|Jinn-Client".

   На экране появится стартовый диалог программы-мастера, позволяющий выбрать средство для набора энтропии — программный модуль генерации или, при наличии ПАК "Соболь", физический датчик устройства.

2. Выберите средство для генерации случайных чисел и нажмите кнопку "Далее >".

На экране появится диалог для ввода параметров запроса.

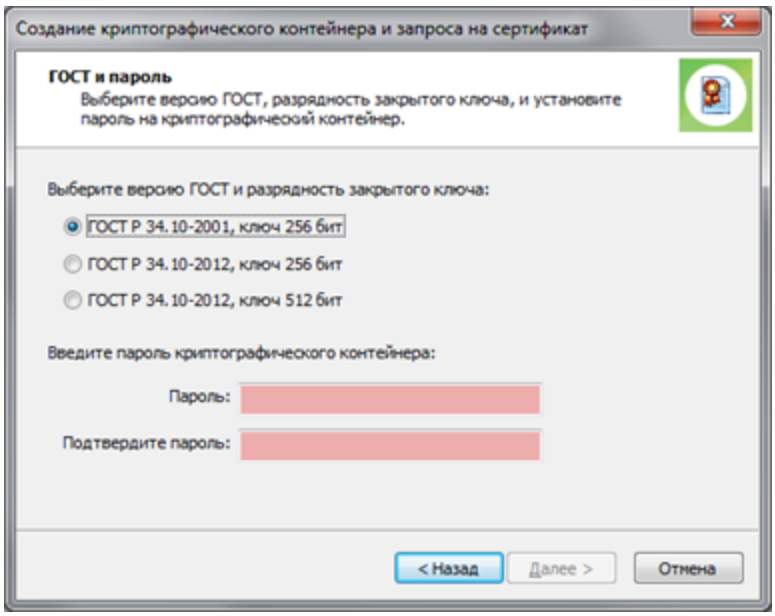


3. Настройте параметры запроса и нажмите кнопку "Далее >".

- В поле "Владелец" выберите из раскрывающегося списка нужное значение.
- В таблице с параметрами укажите нужные параметры владельца сертификата.

> **Совет.** Для ввода значения параметра активируйте щелчком мыши поле в столбце "Значение". Параметры, обязательные для заполнения, отмечены красным цветом.

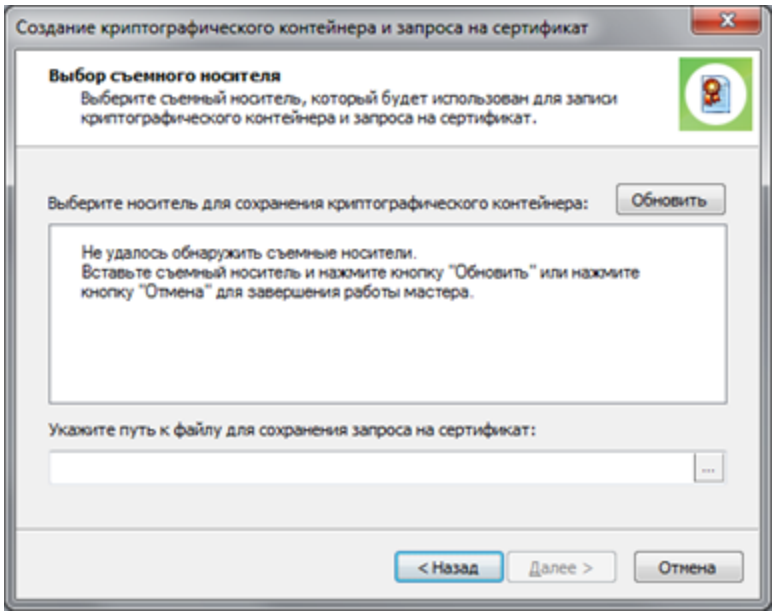
На экране появится диалог для выбора параметров закрытого ключа и ввода пароля доступа к криптографическому контейнеру.



4. Настройте параметры диалога и нажмите кнопку "Далее >".
   - Выберите версию ГОСТ и разрядность, которые будут использоваться при создании закрытого ключа сертификата.
   - Дважды введите пароль, с помощью которого будет защищен доступ к закрытому ключу, хранящемуся в создаваемом контейнере.

   Совет. Запомните или запишите пароль. Этот пароль необходимо сообщить пользователю. Не зная пароля, он не сможет использовать изданный сертификат.

   На экране появится диалог выбора носителя.



5. Выполните следующие действия:
   - в нижнем поле диалога укажите полный путь к файлу, в котором будет сохранен запрос на издание сертификата пользователя;

     Примечание. Для выбора места размещения файла в диалоговом режиме нажмите кнопку "..." в правой части поля.

   - вставьте USB-флеш-накопитель в свободный USB-разъем и нажмите кнопку "Обновить";
   - выберите появившийся в списке диалога накопитель и нажмите кнопку "Далее >".

   На экране появится диалог выбора места хранения резервной копии криптографического контейнера.
6. В поле диалога укажите полный путь к файлу резервной копии создаваемого криптографического контейнера и нажмите кнопку "Далее >".

   Совет. Если резервную копию криптографического контейнера создавать не требуется, оставьте поле пустым и нажмите кнопку "Далее >".

   Далее для создания запроса потребуется генерация набора случайных чисел. При использовании датчика ПАК "Соболь" набор энтропии выполняется автоматически и на экране не отображается. Перейдите к п. 8.

   В противном случае на экране появится окно, предназначенное для накопления энтропии.
7. Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии.
8. В указанной папке будет сформирован файл запроса сертификата, а на носителе будет записан ключевой контейнер. Дождитесь сообщения о завершении процесса создания запроса и закройте его.
9. Извлеките носитель из USB-разъема и нажмите кнопку "Готово".

Глава 3
Управление электронной подписью

Создание электронной подписи в доверенной среде

Использование ПАК "Соболь"

Создание ЭП в доверенной среде выполняется в следующем порядке:

1. Загрузка доверенной среды посредством ПАК "Соболь" (см. ниже).
2. Формирование ЭП (см. стр.**12**).

Внимание! Перед входом в систему отключите от USB-портов компьютера все устройства класса USB Mass Storage Device (флеш-накопители, CD-, DVD-приводы, жесткие диски и т. п.).

Для создания ЭП администратор должен выдать вам:

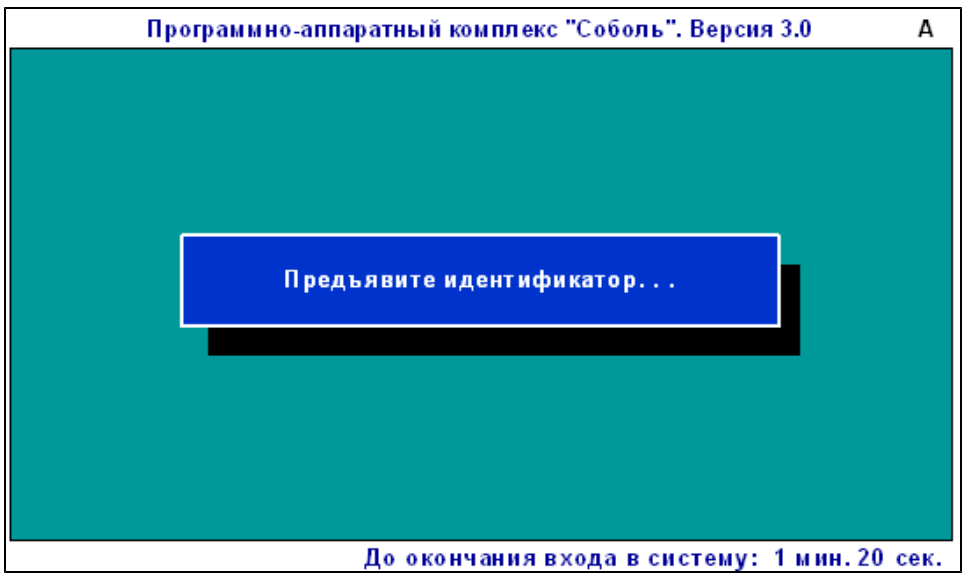
- для входа в ПАК "Соболь":
  - идентификатор iButton/USB-ключ (eToken PRO, eToken PRO (Java), iKey 2032, Рутокен, Рутокен RF)/смарт-карта eToken PRO;
  - пароль;
  - ПИН-код для USB-ключа (eToken PRO, eToken PRO (Java), iKey 2032, Рутокен, Рутокен RF)/смарт-карты eToken PRO;
- для формирования ЭП:
  - ключевой(ые) носитель(и) — USB-флеш-накопитель, USB-ключ (Рутокен, eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash) или смарт-карта (eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ);
  - пароль криптографического контейнера;
  - ПИН-код — для USB-ключа;
  - сертификат ключа и указать место его хранения.

Внимание! Запомните ваши пароли и ПИН-коды, никому их не сообщайте. Никому не передавайте ваш идентификатор, используемый для входа в ПАК "Соболь", и ключевые носители.

Для загрузки доверенной среды:

1. Перезагрузите компьютер или включите питание компьютера, если компьютер был выключен.

   На экране появится окно ПАК "Соболь" с запросом идентификатора.



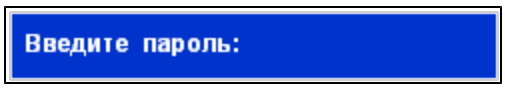
В нижней части окна размещается строка сообщений. В данном случае строка содержит счетчик времени, оставшегося пользователю для предъявления идентификатора и ввода пароля.

2. Предъявите выданный вам идентификатор для входа в ПАК "Соболь".

Примечание.
Предъявите идентификатор — это значит:
- для iButton — плотно приложите идентификатор к считывателю;
- для USB-ключа eToken PRO/eToken PRO (Java)/iKey 2032/Рутокен/Рутокен RF — вставьте идентификатор в свободный USB-разъем компьютера;
- для смарт-карты eToken PRO — вставьте идентификатор в USB-считыватель смарт-карт.

- При использовании USB-идентификатора eToken PRO/eToken PRO (Java) /iKey 2032/Рутокен/Рутокен RF после успешного предъявления идентификатора на экране может появиться окно запроса на ввод ПИН-кода. В этом случае введите ПИН-код (при необходимости уточните у администратора) и нажмите <Enter>.
- Если идентификатор предъявлен неправильно, окно запроса останется на экране. Повторите предъявление идентификатора.

После успешного считывания информации из идентификатора на экране появится диалог для ввода пароля:



3. Введите ваш пароль.

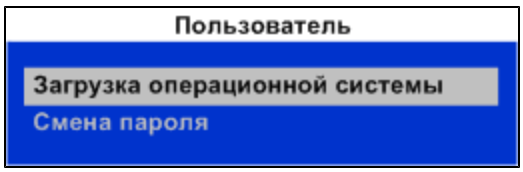
Все введенные символы отображаются знаком "✳". Если при вводе пароля допущены ошибки, вы можете исправить их. Используйте клавиши со стрелками для перемещения курсора, а клавиши <Backspace> или <Delete> для стирания символа. Для отказа от ввода пароля нажмите <Esc>, после чего на экране вновь появится запрос идентификатора.

4. Нажмите <Enter>.

Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и повторите еще раз действия **2** – **4**. Используйте выданный вам идентификатор и не допускайте ошибок при вводе пароля.

Внимание. Учитывайте, что число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение в текущем сеансе входа, то при следующей успешной попытке входа в строке сообщений появится сообщение "Ваш вход в систему запрещен: Вы превысили предел неудачных попыток входа", после чего компьютер будет заблокирован. В этом случае обратитесь за помощью к администратору.

При вводе правильного пароля на экране появится меню пользователя:



5. Выберите команду "Загрузка операционной системы" и нажмите <Enter>.

Начнется загрузка операционной системы компьютера.

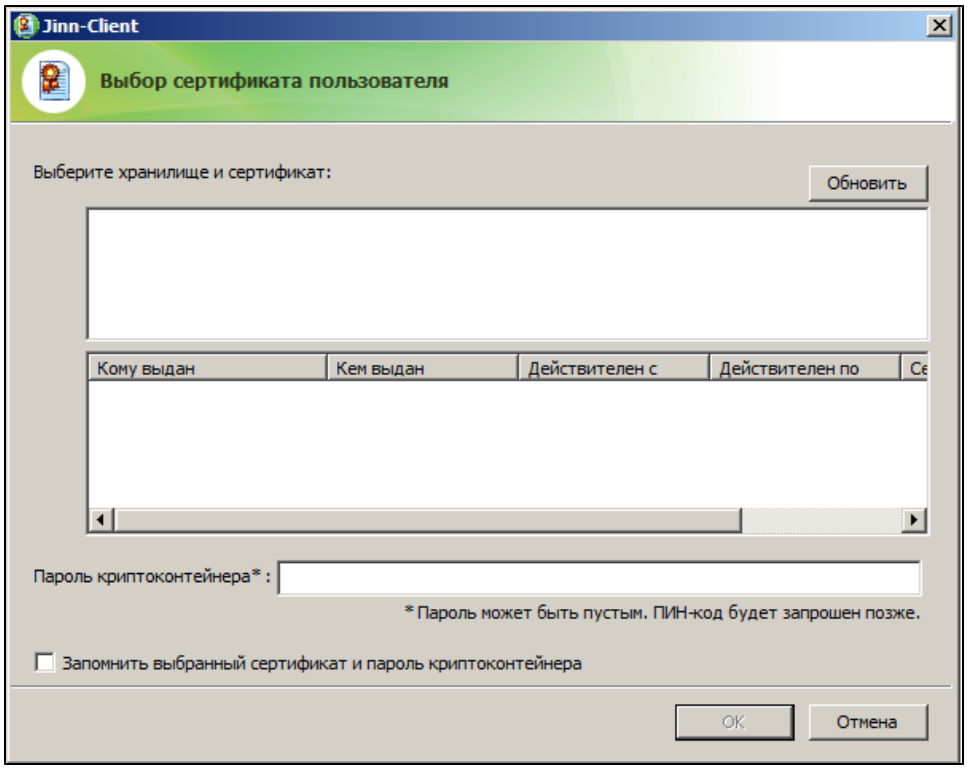
В случае возникновения нештатных ситуаций при входе в систему обратитесь за помощью к администратору.

Для формирования ЭП:

1. Выберите подписываемый документ и перейдите в режим формирования ЭП с помощью ПАК "Jinn".

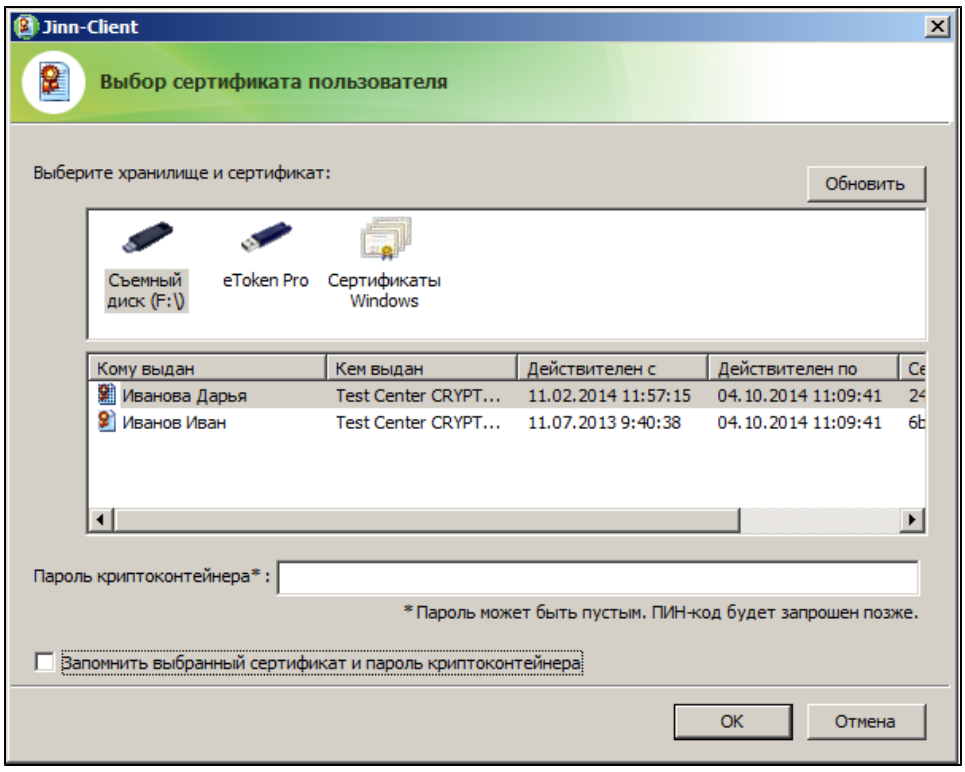
> **Внимание!** В случае появления на экране сообщения "Настройки "Jinn-Client" повреждены. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

На экране появится окно "Выбор сертификата пользователя":



2. Предъявите выданный вам ключевой носитель. Нажмите кнопку "Обновить".

В окне "Выбор сертификата пользователя" появится информация, подобная следующей:



В зависимости от места хранения ключевой информации перейдите к выполнению действия:

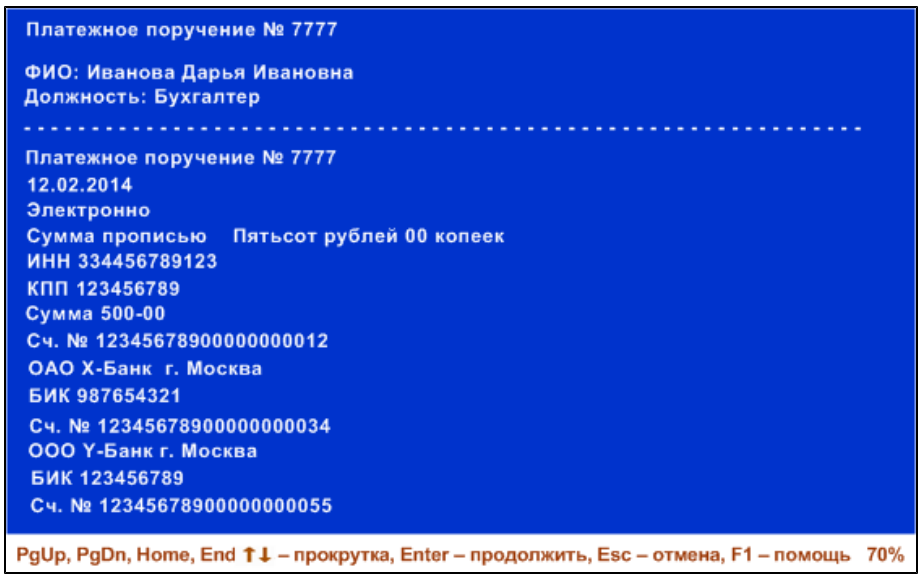
- **3** — при хранении сертификата ключа и ключа подписи на USB-флеш-накопителе;
- **4** — при хранении сертификата ключа и ключа подписи на USB-ключе;
- **5** — при хранении сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе.

3. В случае хранения сертификата ключа и ключа подписи на USB-флеш-накопителе:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-флеш-накопитель и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";

Внимание! Если вы ввели неверный пароль, на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

На экране появится окно с отображением подписываемого документа, подобное следующему:



- перейдите к выполнению действия **6** данной процедуры.

4. В случае хранения сертификата ключа и ключа подписи на USB-ключе:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-ключ и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- в появившееся на экране окне введите значение ПИН-кода (при необходимости уточните его у администратора);

> **Внимание!** При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
>
> При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.
>
> В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

- после появления на экране окна с отображением подписываемого документа (см. рисунок выше) перейдите к выполнению действия **6** данной процедуры.

5. В случае хранения сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе:

- в поле "Выберите хранилище и сертификат" выберите пиктограмму "Сертификаты Windows" и необходимый сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- если администратор выдал вам ПИН-код для USB-ключа, то в появившееся на экране окно введите его значение.

> **Внимание!** При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
>
> При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.
>
> В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

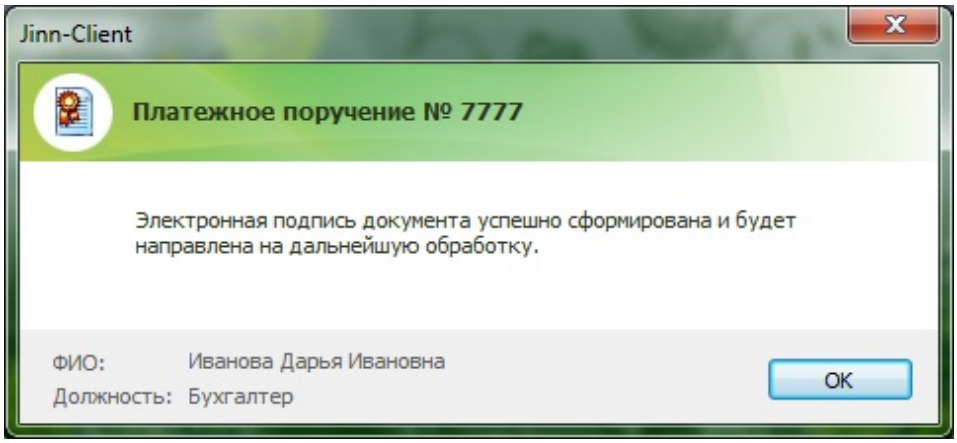
На экране появится окно с отображением подписываемого документа (см. рисунок выше).

6. Для продолжения нажмите <Enter>.

На экране появится запрос:

7. Для формирования ЭП документа нажмите <Enter>, для отмены — <Esc>.

После подписания документа на экране появится следующее окно:



8. Нажмите "ОК".

Использование загрузочного USB-флеш-накопителя

Создание ЭП в доверенной среде с использованием загрузочного USB-флеш-накопителя выполняется в следующем порядке:

1. Загрузка доверенной среды посредством загрузочного USB-флеш-накопителя (см. ниже).
2. Формирование ЭП (см. стр.**15**).

Для создания ЭП администратор должен выдать вам:

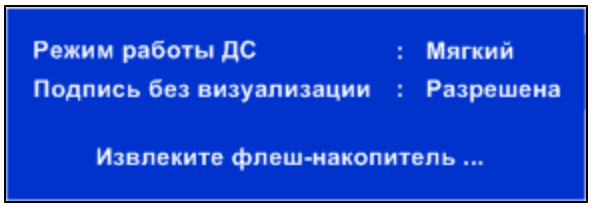
- загрузочный USB-флеш-накопитель;
- ключевой(ые) носитель(и) — USB-флеш-накопитель, USB-ключ (Рутокен, eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash) или смарт-карта (eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ);
- пароль криптографического контейнера;
- ПИН-код — для USB-ключа;
- сертификат ключа и указать место его хранения.

Внимание! Запомните ваш пароль и ПИН-код, никому их не сообщайте. Никому не передавайте ваш загрузочный USB-флеш-накопитель и ключевые носители.

Для загрузки доверенной среды:

1. Вставьте загрузочный USB-флеш-накопитель в свободный USB-разъем. Перезагрузите компьютер или включите питание компьютера, если компьютер был выключен.
2. Запустите BIOS Setup и определите USB-флеш-накопитель первым загрузочным устройством. Сохраните настройку и выйдите из BIOS Setup.

   На экране появится следующее окно:



Пояснение. Режимы работы комплекса можно задавать с помощью клавиш <F9> и <F10>:

- <F9> — "Мягкий"/"Жесткий". Работа комплекса в жестком режиме обеспечивает более совершенную защиту документа при его визуализации. Однако этот режим функционирует не для всех видеокарт, что может вызвать затруднения в работе комплекса. Поэтому рекомендуется использовать мягкий режим. Если же жесткий режим используется в системе, в которой не определен драйвер видеокарты, при визуализации на экране может появиться сообщение "Невозможно получить настройки видеоадаптера". В этом случае необходимо корректно установить драйвер данной видеокарты.
- <F10> — разрешить/запретить подписывать документ без его визуализации. В случае установки запрета подписи без визуализации бинарные документы подписать будет нельзя.

3. Извлеките загрузочный USB-флеш-накопитель.

   Начнется загрузка операционной системы компьютера.

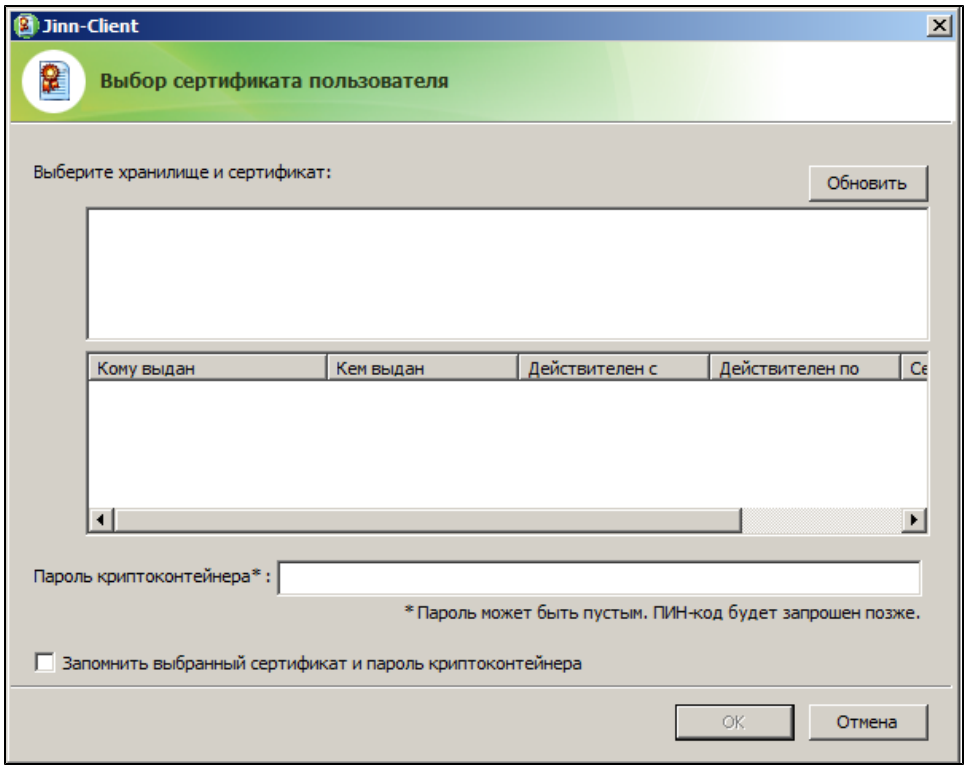
В случае возникновения нештатных ситуаций при входе в систему обратитесь за помощью к администратору.

Для формирования ЭП:

1. Выберите подписываемый документ и перейдите в режим формирования ЭП с помощью ПАК "Jinn".

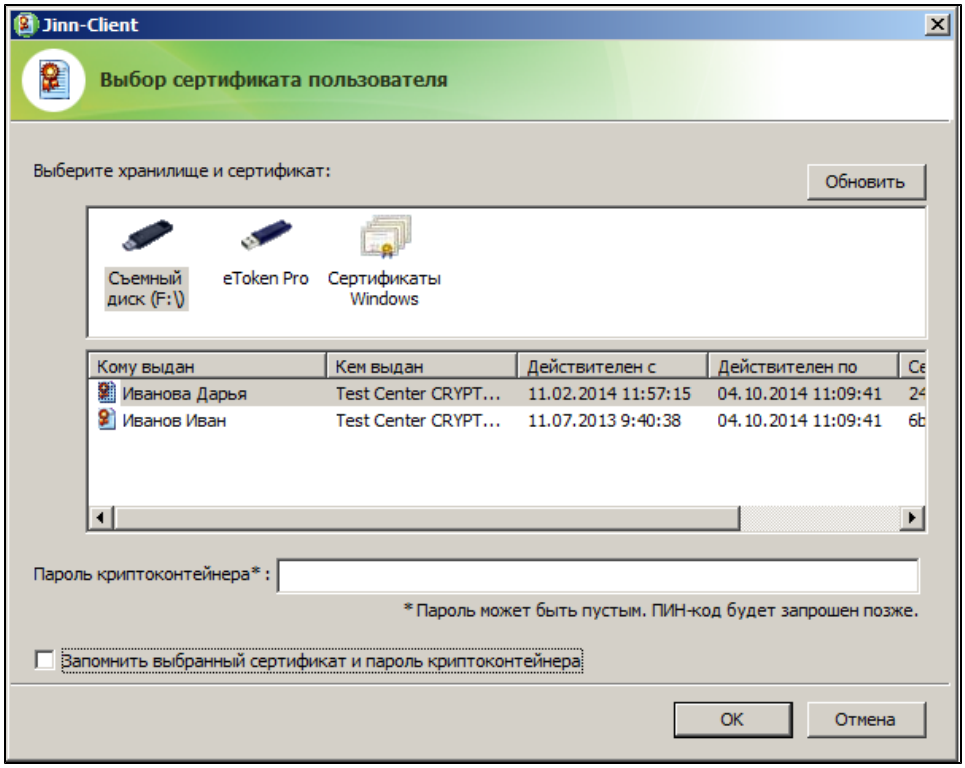
Внимание! В случае появления на экране сообщения "Настройки "Jinn-Client" повреждены. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

На экране появится окно "Выбор сертификата пользователя":



2. Предъявите выданный вам ключевой носитель. Нажмите кнопку "Обновить".

В окне "Выбор сертификата пользователя" появится информация, подобная следующей:



В зависимости от места хранения ключевой информации перейдите к выполнению действия:

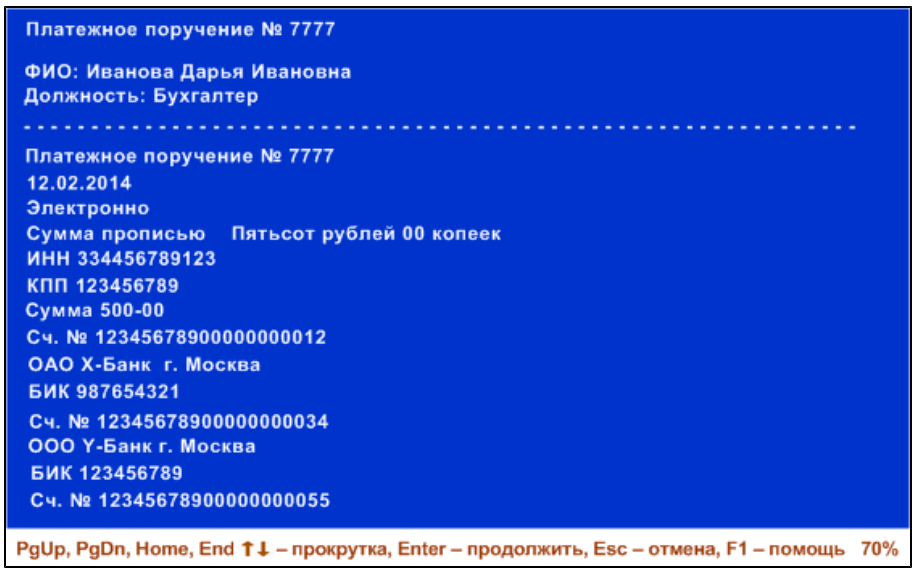
- **3** — при хранении сертификата ключа и ключа подписи на USB-флеш-накопителе;
- **4** — при хранении сертификата ключа и ключа подписи на USB-ключе или смарт-карте;
- **5** — при хранении сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе/смарт-карте.

3. В случае хранения сертификата ключа и ключа подписи на USB-флеш-накопителе:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-флеш-накопитель и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";

Внимание! При вводе неверного пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

На экране появится окно с отображением подписываемого документа, подобное следующему:



- перейдите к выполнению действия **6** данной процедуры.

4. В случае хранения сертификата ключа и ключа подписи на USB-ключе:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-ключ/смарт-карту и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- если администратор выдал вам ПИН-код, то в появившееся на экране окно введите его значение;

> **Внимание!** При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
>
> При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.
>
> В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

- после появления на экране окна с отображением подписываемого документа (см. рисунок выше) перейдите к выполнению действия **6** данной процедуры.

5. В случае хранения сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе/смарт-карте:

- в поле "Выберите хранилище и сертификат" выберите пиктограмму "Сертификаты Windows" и необходимый сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- если администратор выдал вам ПИН-код для USB-ключа, то в появившееся на экране окно введите его значение.

> **Внимание!** При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
>
> При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.
>
> В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

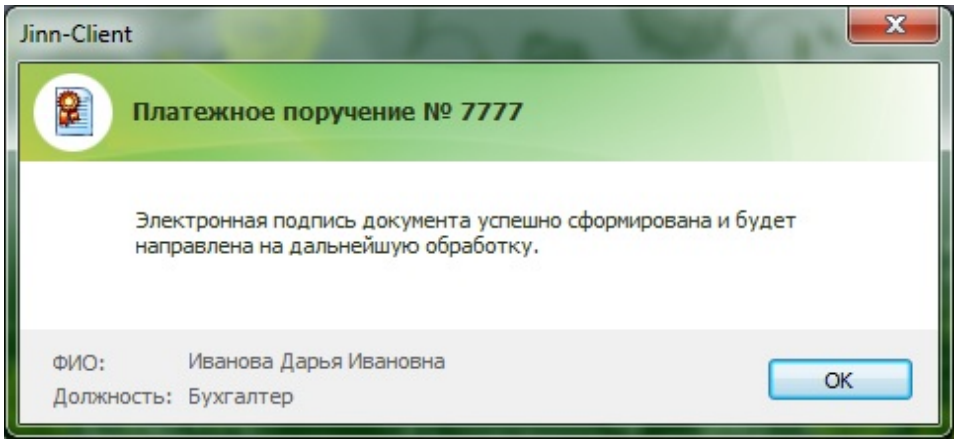
На экране появится окно с отображением подписываемого документа (см. рисунок выше).

6. Для продолжения нажмите <Enter>.

На экране появится запрос:

7. Для формирования ЭП документа нажмите <Enter>, для отмены — <Esc>.

После подписания документа на экране появится следующее окно:



8. Нажмите "ОК".

Создание электронной подписи в среде операционной системы

Для создания ЭП в среде операционной системы администратор должен выдать вам:

- ключевой(ые) носитель(и) — USB-флеш-накопитель, USB-ключ (Рутокен, eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash) или смарт-карта (eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ);
- пароль криптографического контейнера;
- ПИН-код — для USB-ключа/смарт-карты;
- сертификат ключа и указать место его хранения.

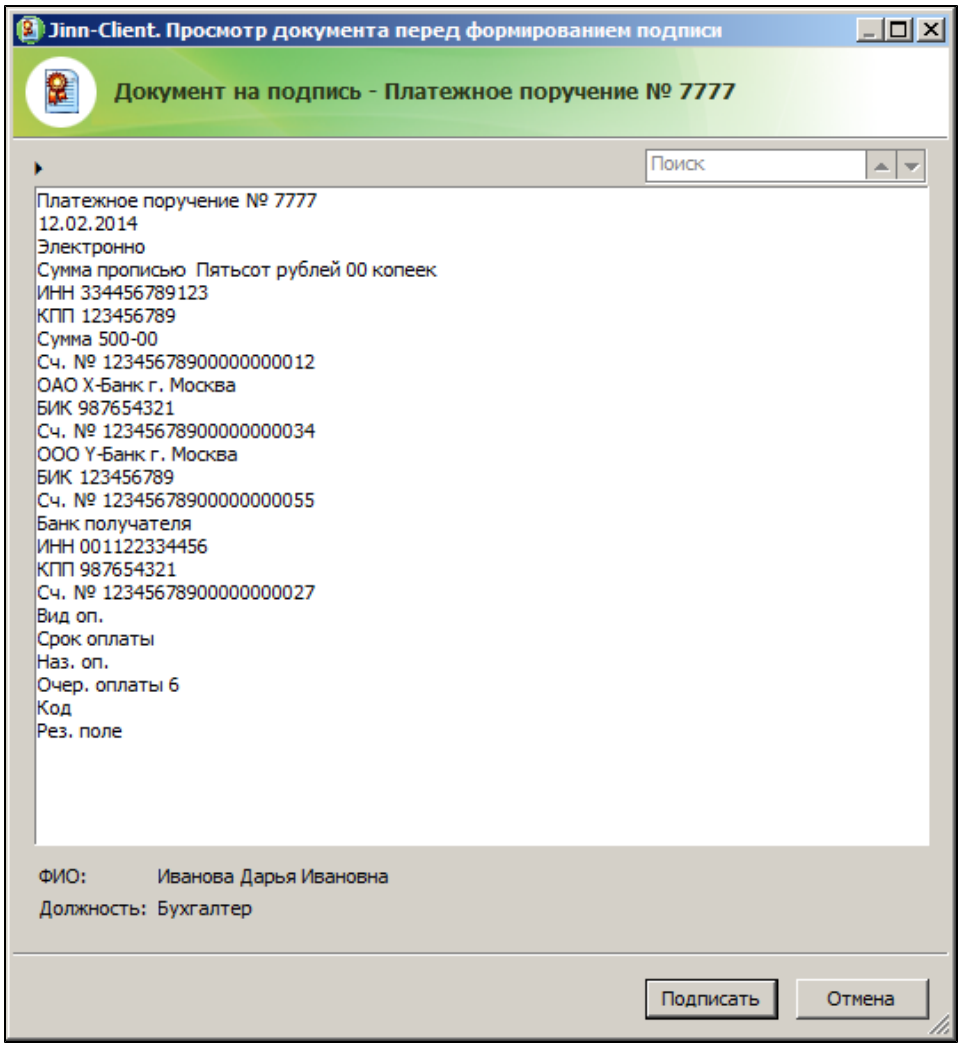
Внимание! Запомните ваш пароль и ПИН-код, никому их не сообщайте. Никому не передавайте ваш персональный USB-флеш-накопитель/USB-ключ/смарт-карту.

Для формирования ЭП:

1. Выберите подписываемый документ и перейдите в режим формирования ЭП с помощью ПАК "Jinn".

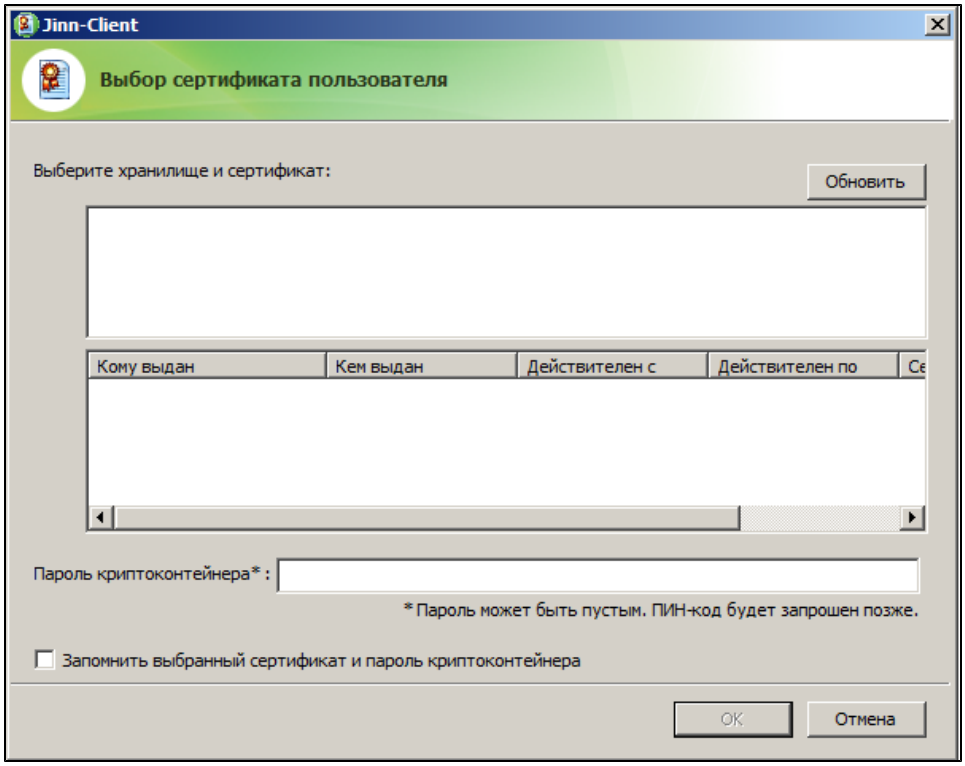
   Внимание! В случае появления на экране сообщения "Настройки "Jinn-Client" повреждены. Необходимо переустановить "Jinn-Client" обратитесь за помощью к администратору.

   На экране появится окно "Документ на подпись" с отображением подписываемого документа.



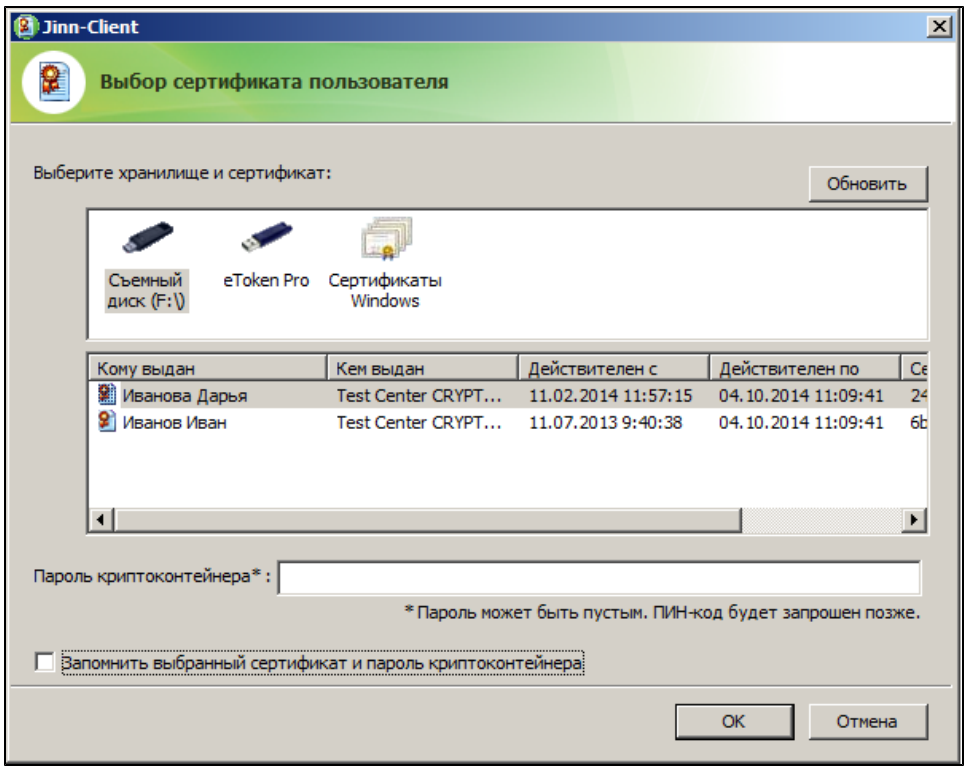
2. Нажмите кнопку "Подписать".

На экране появится окно "Выбор сертификата пользователя":



3. Предъявите ключевой носитель. Нажмите кнопку "Обновить".

В окне "Выбор сертификата пользователя" появится информация, подобная следующей:



В зависимости от места хранения ключевой информации перейдите к выполнению действия:

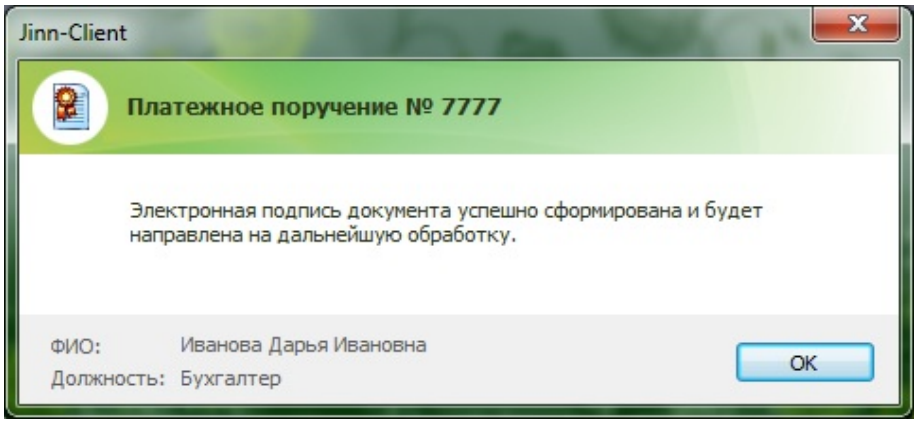
- **4** — при хранении сертификата ключа и ключа подписи на USB-флеш-накопителе;
- **5** — при хранении сертификата ключа и ключа подписи на USB-ключе;
- **6** — при хранении сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе/смарт-карте.

4. В случае хранения сертификата ключа и ключа подписи на USB-флеш-накопителе:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-флеш-накопитель и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";

> **Внимание!** При вводе неверного пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".
> В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

На экране появится следующее окно:



- перейдите к выполнению действия **7** данной процедуры.

5. В случае хранения сертификата ключа и ключа подписи на USB-ключе или смарт-карте:

- в поле "Выберите хранилище и сертификат" выберите необходимые USB-ключ/смарт-карту и сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- если администратор выдал вам ПИН-код, то в появившееся на экране окно введите его значение;

Внимание! При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".

При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.

В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

- после появления на экране окна с сообщением об успешном формировании ЭП документа (см. рисунок выше) перейдите к выполнению действия **7** данной процедуры.

6. В случае хранения сертификата ключа в хранилище Windows и ключа подписи на USB-флеш-накопителе/USB-ключе/смарт-карте:

- в поле "Выберите хранилище и сертификат" выберите пиктограмму "Сертификаты Windows" и необходимый сертификат;
- при необходимости запоминания пути к выбранному сертификату и пароля криптографического контейнера отметьте соответствующее поле (рекомендуется при формировании подписи нескольких документов);
- введите пароль в поле "Пароль криптоконтейнера";
- нажмите "ОК";
- если администратор выдал вам ПИН-код для USB-ключа/смарт-карты, то в появившееся на экране окно введите его значение.

Внимание! При неверном указании сертификата или пароля на экране появится сообщение об ошибке. Для возврата к процедуре выбора сертификата нажмите "Да", в случае отказа — "Нет".

При неверном вводе ПИН-кода на экране появится сообщение об ошибке. Введите правильный ПИН-код.

В случае появления на экране сообщения "Ошибка тестирования программного датчика случайных чисел. Необходимо переустановить "Jinn-Client", создать криптографический контейнер и издать новый сертификат" обратитесь за помощью к администратору.

На экране появится окно с сообщением об успешном формировании ЭП документа (см. рисунок выше).

7. Нажмите "ОК".