



# Личный кабинет

Руководство Абонента

# Содержание

<b>Введение.....</b>	<b>3</b>
О документе.....	3
Для кого предназначен документ .....	3
Соглашения документа.....	3
О Личном кабинете .....	4
Назначение Личного кабинета.....	4
Жизненный цикл запроса на выпуск сертификата .....	4
Системные требования.....	5
Обратная связь.....	5
<b>Начало работы с Личным кабинетом.....</b>	<b>6</b>
Регистрация в Личном кабинете.....	6
Вход в Личный кабинет.....	6
<b>Работа в Личном кабинете .....</b>	<b>8</b>
Создание заявки на получение услуг удостоверяющего центра.....	8
Создание запроса на выпуск сертификата.....	12
Создание запроса на выпуск сертификата с помощью программы ViPNet CSP .....	12
Создание запроса на выпуск сертификата с помощью программы КриптоПро CSP.....	16
Установка сертификата.....	20
Установка сертификата с помощью программы ViPNet CSP.....	20
Установка сертификата с помощью программы КриптоПро CSP .....	21
<b>Глоссарий.....</b>	<b>23</b>

# Введение

## О документе

### Для кого предназначен документ

Данное руководство предназначено для пользователей (далее - Абонент) Личного кабинета на веб-сайте компании «ИнфоТеКС Интернет Траст». В нем содержится подробная информация о процедурах, необходимых для создания запросов на выпуск сертификатов.

### Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях




Обозначение	Описание
	<b>Внимание!</b> Указывает на обязательное для исполнения или следования действие или информацию.
	<b>Примечание.</b> Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	<b>Совет.</b> Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
<b>Название</b>	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
<b>Клавиша+Клавиша</b>	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
<b>Меню &gt; Подменю &gt; Команда</b>	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
<b>Код</b>	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

# О Личном кабинете

## Назначение Личного кабинета

Личный кабинет — это ваш индивидуальный раздел на сайте «Инфотекс Интернет Траст». Вы получаете приглашение зарегистрироваться в нем от организаций-партнеров УЦ ИИТ (далее - Агент). С помощью своего Личного кабинета вы можете создать запрос на выпуск сертификата, в режиме реального времени проследить за его выполнением, а также получить сертификат после того, как запрос пройдет верификацию (см. глоссарий, стр. 22).

Личный кабинет призван максимально ускорить и упростить процесс подачи запроса на выпуск сертификата и получения сертификата.

## Жизненный цикл запроса на выпуск сертификата

Основным сценарием работы с Личным кабинетом является создание и обработка запроса на выпуск сертификата. Жизненный цикл такого запроса представлен на рисунке ниже:

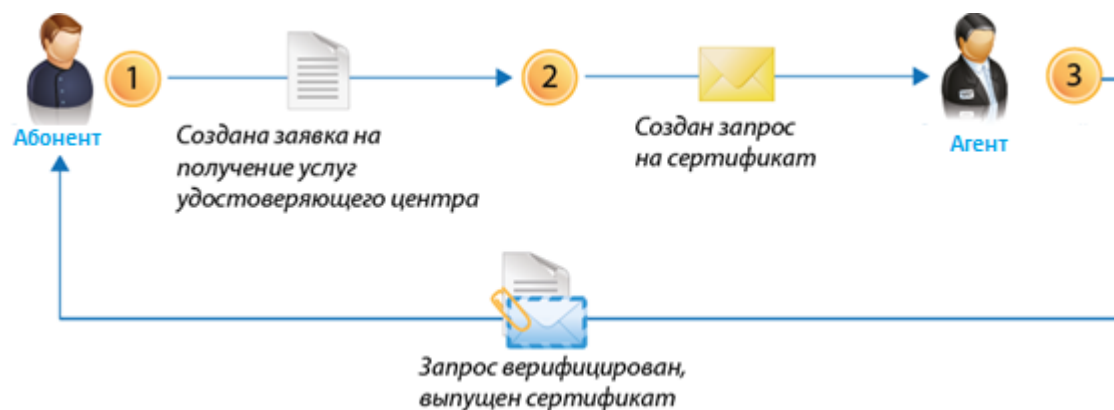


Рисунок 1. Жизненный цикл запроса на выпуск сертификата

Работа с запросом на выпуск сертификата происходит в следующем порядке:

- 1 Абонент создает заявку на получение услуг удостоверяющего центра.
- 2 Абонент в рамках этой заявки создает запрос на сертификат.
- 3 Агент верифицирует запрос и издается сертификат.

# Системные требования

Требования к компьютеру для работы с Личным кабинетом:

- Браузеры:
  - Internet Explorer 10 или более поздней версии;
  - Google Chrome актуальной версии;
  - Mozilla Firefox актуальной версии.
- Криптопровайдеры:
  - ViPNet CSP последней доступной версии  
[http://infotecs.ru/downloads/product\\_full.php?id\\_product=2096;](http://infotecs.ru/downloads/product_full.php?id_product=2096)
  - КриптоПро CSP последней доступной версии;
  - JCrypto последней доступной версии;
  - криптопровайдеры, встроенные в токен (см. глоссарий, стр. 22).
- Дополнительное ПО:
  - JavaLSS;



**Примечание.** Если на вашем компьютере не установлено необходимое дополнительное ПО, его установка будет предложена в процессе работы в Личном кабинете.

---

## Обратная связь

Для решения возникающих проблем обратитесь в службу технической поддержки компании «ИнфоТекС Интернет Траст».

- Электронный адрес службы поддержки <mailto:SupportIT@iitrust.ru>.
- Форма запроса в службу технической поддержки <http://www.iitrust.ru/support/request.php>.
- +7 (495) 737-33-69 — «горячая линия» службы технической поддержки.
- 8 800 250-02-65 — бесплатный звонок из любого региона России (кроме Москвы).
- Онлайн чат, доступный в правом нижнем углу на официальном сайте компании [www.iitrust.ru](http://www.iitrust.ru)

# Начало работы с Личным кабинетом

## Регистрация в Личном кабинете

Для начала работы с Личным кабинетом вам не нужно проходить отдельную процедуру регистрации. Если у вас еще нет учетной записи для входа в Личный кабинет, то она будет создана автоматически в процессе создания запроса на выпуск сертификата (см. «Создание заявки на получение услуг удостоверяющего центра» на стр. 8).

## Вход в Личный кабинет

После входа в Личный кабинет вы можете просмотреть свои заявки и создать запрос на выпуск сертификата (см. «Создание запроса на выпуск сертификата» на стр. 12).

Чтобы войти в Личный кабинет, перейдите на его веб-страницу по уникальной реферальной ссылке, полученной от Агента, вида <https://iitrust.lk/api/agent/ref/.../>, и выполните следующие действия:

- 1 Щелкните ссылку **Личный кабинет**.



Рисунок 2. Ссылка «Личный кабинет»

- 2 Введите логин и пароль в соответствующие поля. Если вы еще не зарегистрированы, пройдите регистрацию при подаче запроса на получение услуг удостоверяющего центра (см. «Создание заявки на получение услуг удостоверяющего центра» на стр. 8).

3 Нажмите кнопку **Войти**.

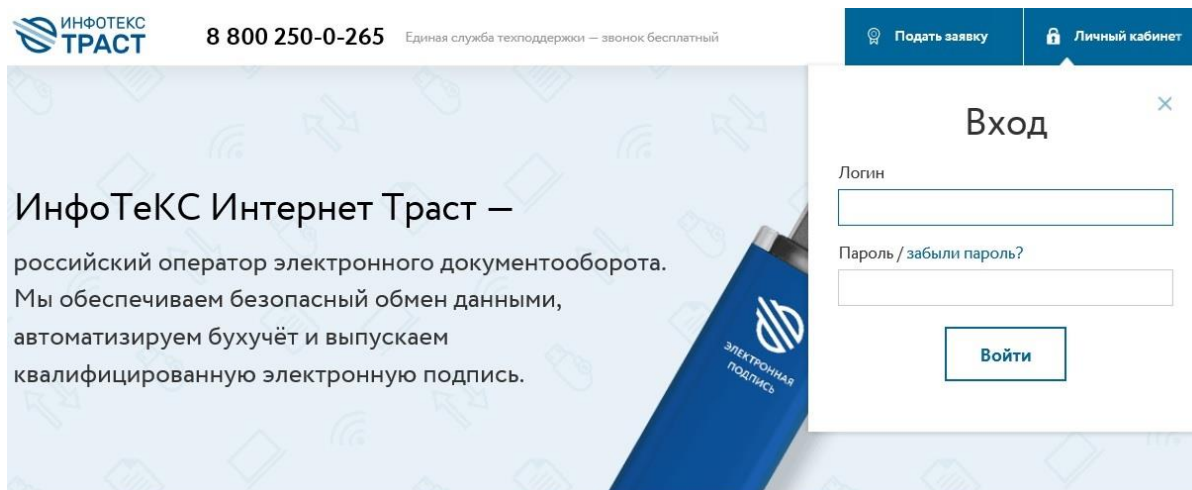


Рисунок 3. Страница входа в Личный кабинет

# Работа в Личном кабинете

Процесс получения сертификата с помощью Личного кабинета состоит из двух этапов:

- 1 Создание заявки на получение услуг удостоверяющего центра (на стр. 8).
- 2 Создание запроса на выпуск сертификата (на стр. 12).

## Создание заявки на получение услуг удостоверяющего центра

Чтобы создать заявку на получение услуг удостоверяющего центра, выполните следующие действия:

- 1 Если вы уже получали логин и пароль для своего Личного кабинета, войдите в Личный кабинет (см. «Вход в Личный кабинет» на стр. 6), иначе, получите уникальную реферальную ссылку на Личный кабинет от Агента, вида <https://iitrust.lk/api/agent/ref/.../>, и перейдите по ней на страницу Личного кабинета.
- 2 На главной странице сайта Личного кабинета, в разделе **Заказать электронную подпись**, выберите тип сертификата, который Вы хотите получить.

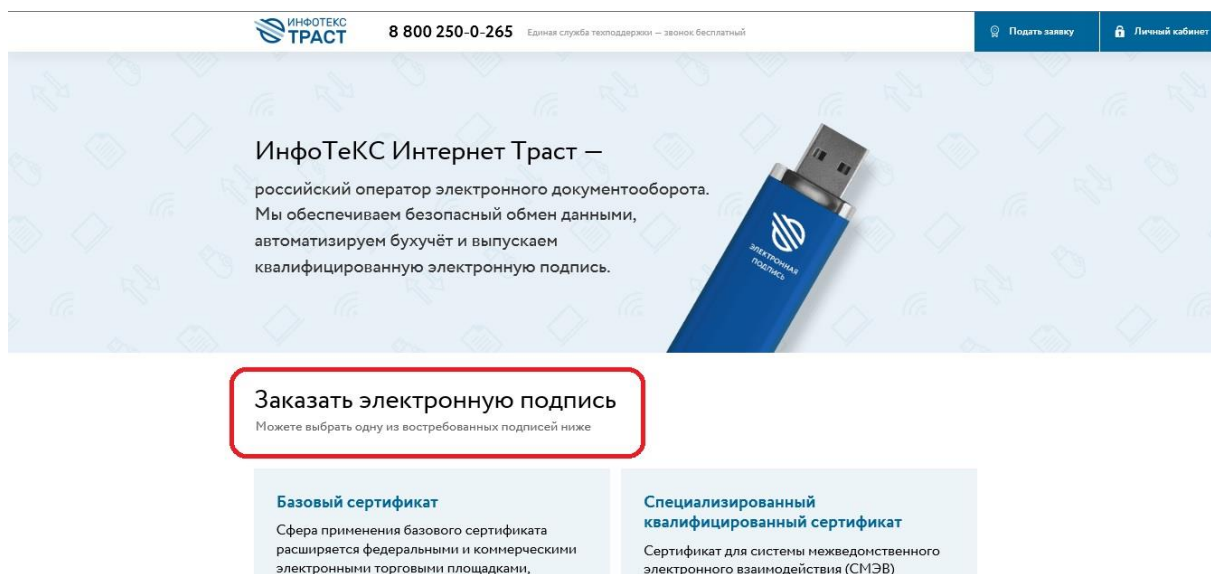


Рисунок 4. Выбор типа сертификата в разделе «Заказать электронную подпись»

- 3 **Шаг 1.** Отметьте галочками желаемую сферу применения сертификата. Справа отображается общая стоимость сертификата. Выберите тип заявителя и нажмите кнопку «**Продолжить**».



# Оформление

Сертификат

Реквизиты

Личные данные

Точка выдачи

## Базовый сертификат

Расширение сферы применения базового сертификата под электронные торговые площадки

Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, ММВБ, zakazrf.ru

Тип полномочий для ФЭТП

Администратор организации

Уполномоченный специалист

Специалист с правом подписи контракта

Ассоциация ЭТП (включая группу площадок B2B, uTender)

uTender

Группа площадок B2B

Сибирская торговая площадка

Сдача отчетности через портал nalog.ru

Электронная торговая площадка ГПБ (etp.gpb.ru)

ФСТ

Центр реализации

Рисунок 5. Выбор сфер применения сертификата

Заполнено: 1 из 4

**Ваш заказ**

Базовый сертификат

Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, ММВБ, zakazrf.ru

Ассоциация ЭТП (включая группу площадок B2B, uTender)

uTender

Группа площадок B2B

Центр реализации

**Всего 7 100 ₽**



Напишите нам, мы онлайн!



**Внимание!** При выборе услуги Портал Росреестра необходимо указать полномочия (субъекты правоотношений). С ограничениями использования сертификата можно ознакомиться в **Приложении IV к распоряжению Федеральной службы государственной регистрации, кадастра и картографии от 27.03.2014 № Р/32** <https://rosreestr.ru/site/activity/docs/detail.php?ID=6257>

- 4 **Шаг 2.** Заполните необходимые реквизиты в зависимости от типа Абонента (ЮЛ, ИП, ФЛ) и нажмите кнопку «**Продолжить**».

**Оформление**

Сертификат **Реквизиты** Личные данные Точка выдачи

Организация

ИНН

Если вы не знаете ИНН своей организации, то можете его найти на сайте ФНС.

КПП

**Юридический адрес**

Регион

Город

Улица

Дом

Заполнено: **1 из 4**

**Ваш заказ**

Базовый сертификат

Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, ММВБ, zakazrf.ru

Ассоциация ЭТП (включая группу площадок B2B, uTender)

uTender

Группа площадок B2B

Центр реализации

**Всего 7 100 ₽**

Напишите нам, мы онлайн!

Рисунок 6. Заполнение реквизитов в запросе на получение услуг удостоверяющего центра на примере юридического лица.

- 5 Шаг 3. Заполните личные данные владельца сертификата и нажмите кнопку «Продолжить»

**Оформление**

Сертификат Реквизиты **Личные данные** Точка выдачи

**Владелец сертификата**

Фамилия

Имя

Отчество

✕ Отчество отсутствует

СНИЛС

Мобильный телефон

Должность

Электронная почта

На эту почту придет логин и пароль для личного кабинета и она будет использована для оформления сертификата. Если вы желаете оставить ее конфиденциальной – добавьте ниже другую почту для отображения в открытой части электронной подписи.

Заполнено: **2 из 4**

**Ваш заказ**

Базовый сертификат

Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, ММВБ, zakazrf.ru

Ассоциация ЭТП (включая группу площадок B2B, uTender)

uTender

Группа площадок B2B

Центр реализации

**Всего 7 100 ₽**

Напишите нам, мы онлайн!

Рисунок 7. Заполнение личных данных в запросе на получение услуг удостоверяющего центра на примере юридического лица.

- 6 Если в сертификате Вы хотите указать адрес электронной почты, отличный от указанного в разделе **Владелец сертификата**, то добавьте новый адрес электронной почты для сертификата.

Электронная почта

На эту почту придет логин и пароль для личного кабинета и она будет использована для оформления сертификата. Если вы желаете оставить ее конфиденциальной — добавьте ниже другую почту для отображения в открытой части электронной подписи.

+ Добавить электронную почту для сертификата

+ Добавить контактное лицо

Рисунок 8. Ввод адреса электронной почты для сертификата

- 7 Выберите точку выдачи сертификата (см. глоссарий, стр. 23) и нажмите кнопку **Оформить заявку**.

## Оформление

Сертификат   Реквизиты   Личные данные   **Точка выдачи**

Регион

Точки выдачи

- ОАО "ИнфоТеКС Интернет Траст", г. Москва  
127287, г. Москва, Старый Петровско-Разумовский проезд, 1/23, стр. 1, этаж 2  
+7 (495) 737-93-72  
lkitrust@gmail.com
- Воронеж 2  
ул. Хомяков, 1, дом. 1  
lkitrust@gmail.com
- Филиал Краснодарского края  
ул. Тестовая д.3  
lkitrust@gmail.com

Заполнено: **3 из 4**

### Ваш заказ

Базовый сертификат

Федеральные ЭТП – РТС-тендер, Сбербанк-АСТ, ЕЭТП, ММВБ, zakazrf.ru

Ассоциация ЭТП (включая группу площадок B2B, uTender)

Рисунок 9. Выбор точки выдачи сертификата

Нажмите кнопку **«Продолжить»**.

Появится информационное сообщение о том, что заявка успешно оформлена! После создания заявки Вам придет письмо на Ваш адрес электронной почты.

Если Вы создавали заявку впервые, то Вы получите на электронную почту логин и пароль для входа в Личный кабинет (см. «Вход в Личный кабинет» на стр. 6). Теперь вы можете войти в Личный кабинет и создать запрос на сертификат (см. «Создание запроса на выпуск сертификата» на стр. 12).

# Создание запроса на выпуск сертификата

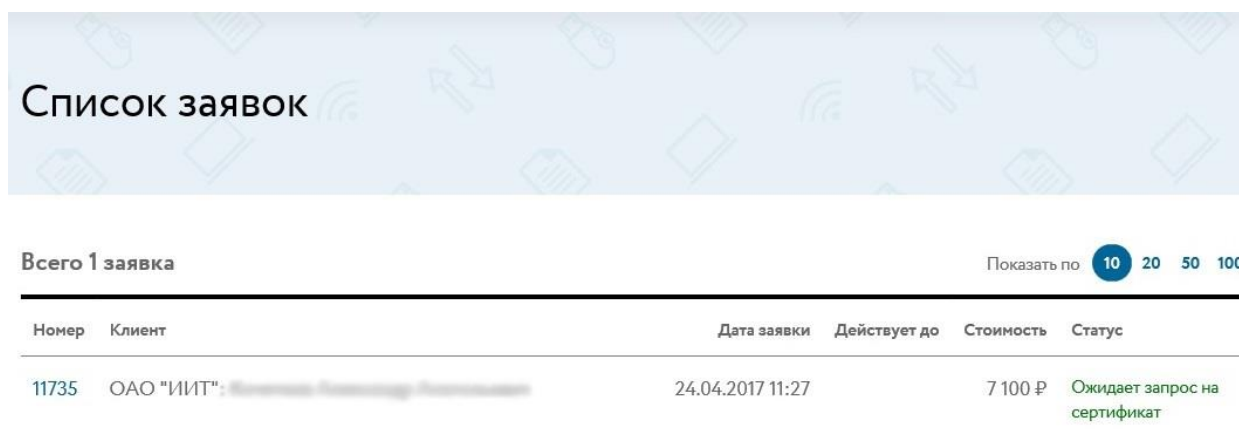
После того, как Вы создали заявку на получение услуг удостоверяющего центра (см. «Создание заявки на получение услуг удостоверяющего центра» на стр. 8), вы можете создать запрос на выпуск сертификата. Для этого выполните действия в зависимости от установленного на вашем компьютере криптопровайдера:

- Создание запроса на выпуск сертификата с помощью программы ViPNet CSP (на стр. 12).
- Создание запроса на выпуск сертификата с помощью программы КриптоПро CSP (на стр. 15).

## Создание запроса на выпуск сертификата с помощью программы ViPNet CSP

Чтобы создать запрос на выпуск сертификата с помощью программы ViPNet CSP, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. «Вход в Личный кабинет» на стр. 6).
- 2 После входа в Личный кабинет Вы увидите список ваших заявок.



Номер	Клиент	Дата заявки	Действует до	Стоимость	Статус
11735	ОАО "ИИТ": <small>Информационные Технологии</small>	24.04.2017 11:27		7 100 ₽	Ожидает запрос на сертификат

Рисунок 10. «Список заявок»


- 3 После обработки заявки Агентом счет отправляется вам на электронную почту (статусы заявки **Проверка данных** и **Ожидает оплату**). После поступления оплаты статус заявки поменяется на **Ожидает запрос на сертификат**.
- 4 Выберите заявку в статусе **Ожидает запрос на сертификат** и щелкните на её строчку/номер.
- 5 Если Вы видите сообщение о необходимости установки дополнительного ПО, выполните его установку, перейдя по ссылке. Если JavaLSS установлен, то необходимо его запустить через **Пуск - InfoTeCS – JLSS**. В нижнем правом углу, рядом с датой должен появиться значок 



Рисунок 11. Сообщение о необходимости установки/запуска дополнительного ПО

- 6 Нажмите кнопку **Сгенерировать запрос на сертификат**.

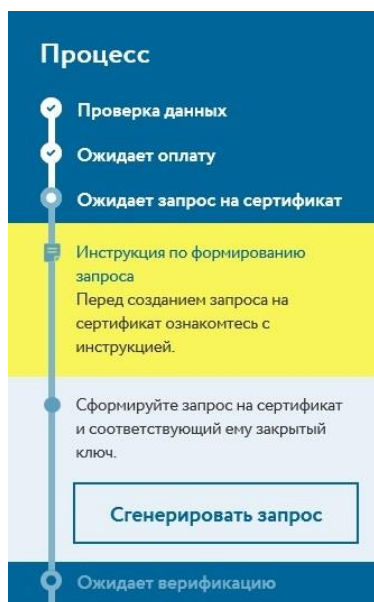


Рисунок 12. Создание запроса на сертификат

- 7 Если Вы хотите прочитать инструкцию по созданию запроса на выпуск сертификата, щелкните ссылку, которая ведет на руководство для криптопровайдера, который установлен на Вашем компьютере.



**Внимание!** Далее в этом разделе описано создание контейнера ключей в программе ViPNet CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 8 Откроется окно **Создание ключа электронной подписи**. Выберите криптопровайдер для генерации запроса. Если на ПК установлен ViPNet CSP, выбирайте Infotecs Cryptographic Service Provider.

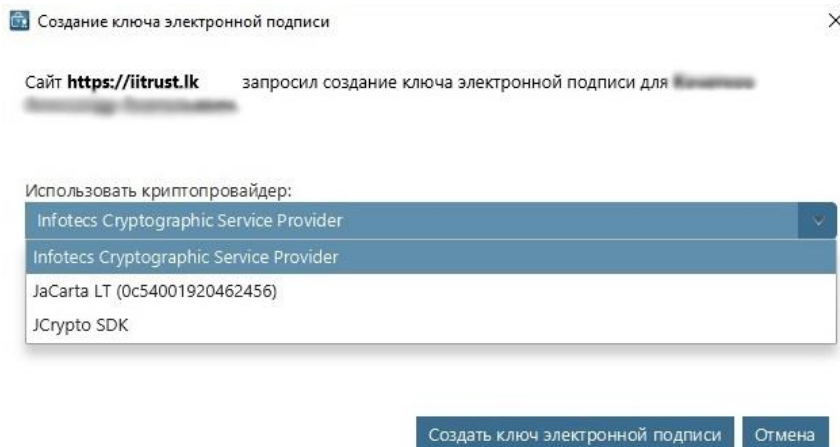


Рисунок 13. Выбор криптопровайдера для создания ключа электронной подписи

- 9 Откроется окно **Инициализация контейнера ключей программы ViPNet CSP**. Выберите место хранения контейнера ключей и нажмите кнопку **ОК**.

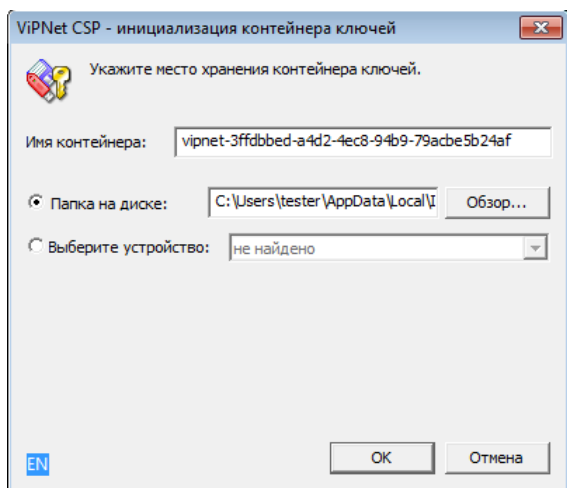


Рисунок 14. Окно выбора места хранения контейнера ключей программы ViPNet CSP

---

**Примечание.** Если не указывали собственный путь, то контейнер ключа по умолчанию создается на жестком диске в каталоге:



- C:\Users\[имя учетной записи]\AppData\Local\InfoteCS\Containers – В ОС Windows 7 и выше
- C:\Documents and Settings\[имя учетной записи]\Local Settings\Application Data\InfoteCS\Containers – В ОС Windows XP

- 
- 10 В окне создания пароля программы ViPNet CSP введите пароль и его подтверждение. Установите флажок **Сохранить пароль**, если не хотите вводить пароль на следующем шаге. Нажмите кнопку **ОК**.

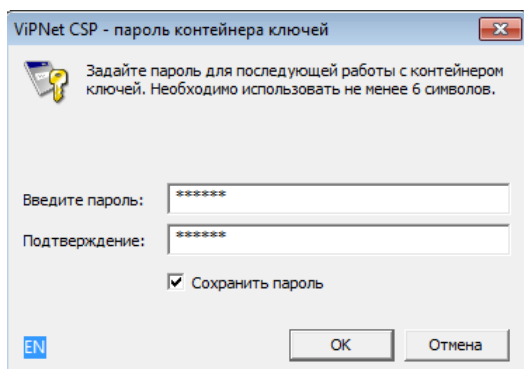


Рисунок 15. Создание пароля контейнера ключей в программе ViPNet CSP



**Внимание!** Обязательно запомните введенный пароль. В случае если пароль будет утерян (забыт), доступ к ключевой информации будет невозможен, что, в свою очередь, приведет к внеплановой смене ключевого дистрибутива

- 11 Появится электронная рулетка (см. глоссарий, стр. 22). Поводите указателем в пределах окна **Электронная рулетка**.

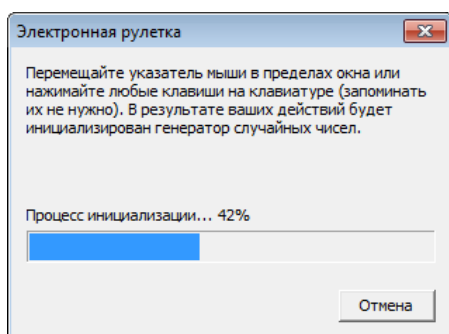


Рисунок 16. Электронная рулетка

- 12 Если при создании пароля доступа к контейнеру ключей Вы не отметили флажок **Сохранить пароль**, в следующем окне введите пароль. Установите флажок **Сохранить пароль**, если не хотите в дальнейшем вводить пароль к этому контейнеру ключей. Нажмите кнопку **ОК**.

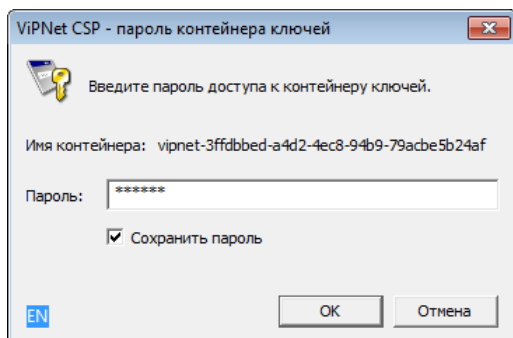


Рисунок 17. Окно ввода пароля к контейнеру ключей в программе ViPNet CSP

13 Ваша заявка получит статус **Ожидает верификацию**.



Рисунок 18. Ожидание верификации запроса Агентом

14 Как только Ваша заявка пройдет верификацию Агентом (см. глоссарий, стр. 22), и сертификат будет издан, статус изменится на **Ожидает завершения**.

15 Агент в своем Личном кабинете нажимает кнопку **Завершить** и Вы сможете установить сертификат (см. «[Установка сертификата](#)» на стр. 20).

## Создание запроса на выпуск сертификата с помощью программы КриптоПро CSP

Чтобы создать запрос на выпуск сертификата с помощью программы КриптоПро CSP, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. «[Вход в Личный кабинет](#)» на стр. 6).
- 2 После входа в Личный кабинет Вы увидите список ваших заявок.

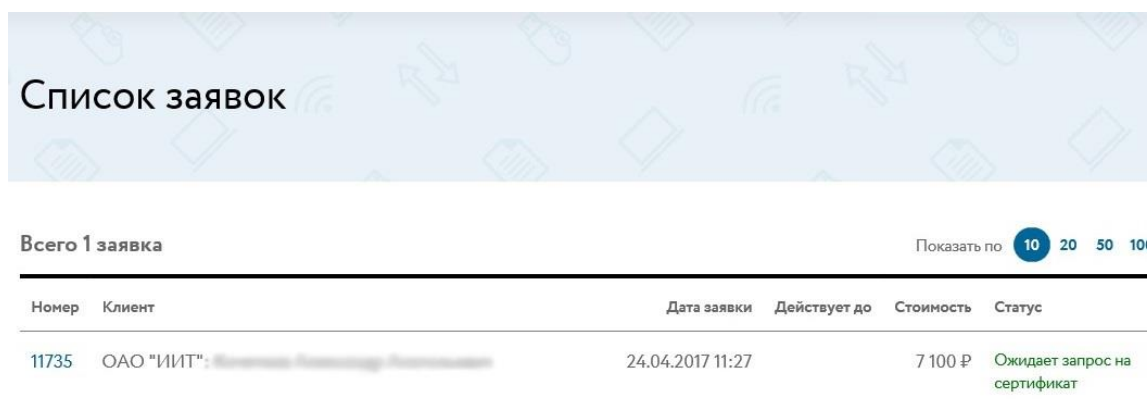


Рисунок 19. «Список заявок»


- 3 После обработки заявки Агентом счет отправляется вам на электронную почту (статусы заявки **Проверка данных** и **Ожидает оплату**). После поступления оплаты статус заявки поменяется на **Ожидает запрос на сертификат**.
- 4 Выберите заявку в статусе **Ожидает запрос на сертификат** и щелкните на её строчку/номер.
- 5 Если Вы видите сообщение о необходимости установки дополнительного ПО, выполните его установку, перейдя по ссылке. Если JavaLSS установлен, то необходимо его запустить через **Пуск - InfoTeCS – JLSS**. В нижнем правом углу, рядом с датой должен появиться значок 





Рисунок 20. Сообщение о необходимости установки/запуска дополнительного ПО

- 6 Нажмите кнопку **Сгенерировать запрос на сертификат**.

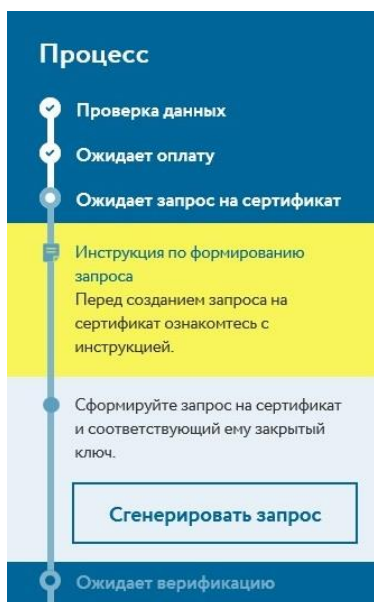


Рисунок 21. Создание запроса на сертификат

- 7 Если Вы хотите прочитать инструкцию по созданию запроса на выпуск сертификата, щелкните ссылку, которая ведет на руководство для криптопровайдера, который установлен на Вашем компьютере.



**Внимание!** Далее в этом разделе описано создание контейнера ключей в программе КриптоПро CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 8 Откроется окно **Создание ключа электронной подписи**. Выберите криптопровайдер для генерации запроса. Выбирайте Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider.

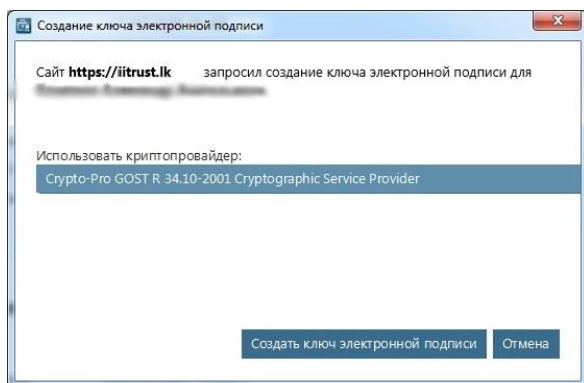


Рисунок 22. Выбор криптопровайдера для создания ключа электронной подписи

- 9 Откроется окно программы КристоПро CSP. Выберите место хранения контейнера ключей и нажмите кнопку **ОК**.

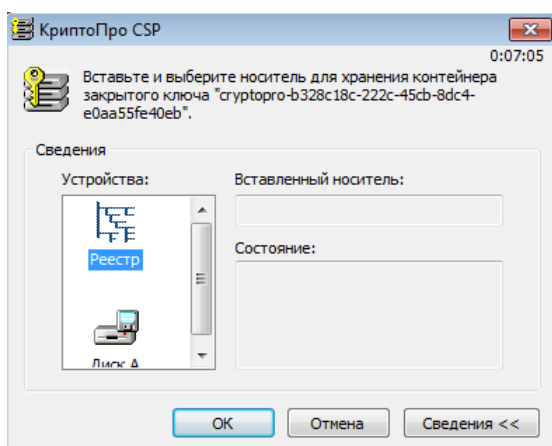


Рисунок 23. Окно выбора места хранения контейнера ключей программы КристоПро CSP

- 10 Появится электронная рулетка (см. глоссарий, стр. 23). Поводите указателем в пределах окна электронной рулетки.

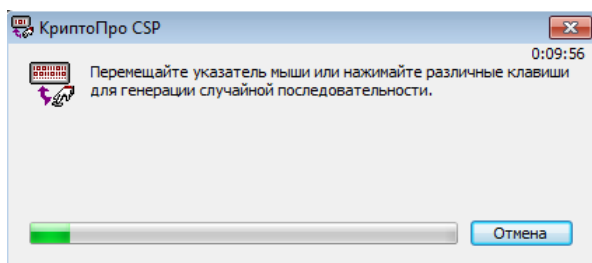


Рисунок 24. Окно электронной рулетки программы КристоПро CSP

- 11 В окне создания пароля программы КристоПро CSP введите пароль и его подтверждение. Нажмите кнопку **ОК**.

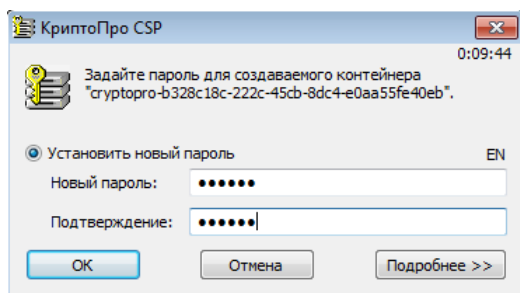


Рисунок 25. Окно задания пароля программы КриптоПро CSP



**Внимание!** Обязательно запомните введенный пароль. В случае если пароль будет утерян (забыт), доступ к ключевой информации будет невозможен, что, в свою очередь, приведет к внеплановой смене ключевого дистрибутива

- 12 Введите пароль доступа к контейнеру ключей. Установите флажок **Запомнить пароль**, если не хотите в дальнейшем не вводить пароль к этому контейнеру ключей. Нажмите кнопку **OK**.

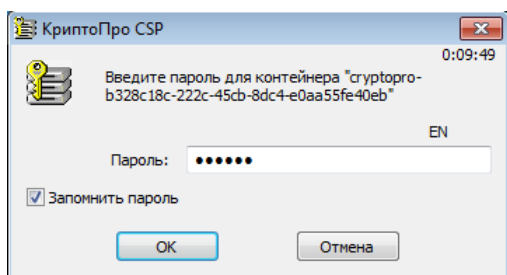


Рисунок 26. Окно ввода пароля к контейнеру ключей программы КриптоПро CSP

- 13 Ваша заявка получит статус **Ожидает верификацию**.



Рисунок 27. Ожидание верификации запроса Агентом

- 14 Как только Ваша заявка пройдет верификацию Агентом (см. глоссарий, стр. 22), и сертификат будет издан, статус изменится на **Ожидает завершения**.
- 15 Агент в своем Личном кабинете нажимает кнопку **Завершить** и Вы сможете установить сертификат (см. «Установка сертификата» на стр. 20).

# Установка сертификата

После того, как по вашему запросу (см. «Создание запроса на выпуск сертификата» на стр. 12) будет издан сертификат, Вы сможете установить его. Для этого выполните действия в зависимости от установленного на вашем компьютере криптопровайдера:

- [Установка сертификата с помощью программы ViPNet CSP](#) (на стр. 20).
- [Установка сертификата с помощью программы КриптоПро CSP](#) (на стр. 21).

## Установка сертификата с помощью программы ViPNet CSP

Чтобы установить сертификат с помощью программы ViPNet CSP, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. «Вход в Личный кабинет» на стр. 6).
- 2 В списке заявок выберите заявку в статусе **Завершена** и нажмите на ее номер/строчку.

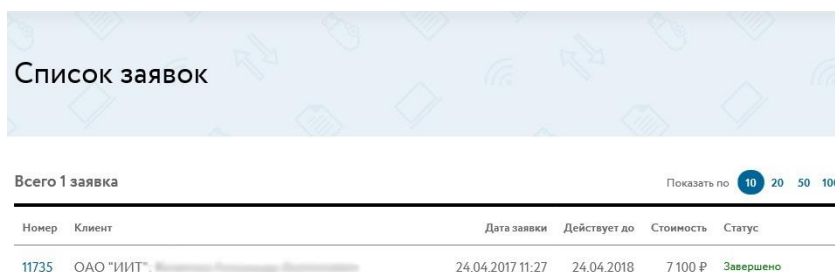


Рисунок 28. Выбор заявки со статусом «Завершена»

- 3 На странице заявки нажмите кнопку **Установить**.



**Внимание!** Далее в этом разделе описано добавление сертификата в контейнер ключей программы ViPNet CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 4 Если при создании пароля доступа к контейнеру ключей Вы не отметили флажок **Сохранить пароль**, в следующем окне введите пароль. Установите флажок **Сохранить пароль**, если не хотите в дальнейшем вводить пароль к этому контейнеру ключей. Нажмите кнопку **ОК**.

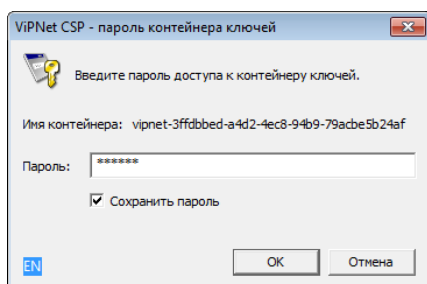


Рисунок 29. Окно ввода пароля к контейнеру ключей в программе ViPNet CSP

- 5 Если Вы ввели верный пароль, то Вы увидите сообщение об успешной установке сертификата.



Рисунок 30. Сертификат успешно установлен

## Установка сертификата с помощью программы КриптоПро CSP

Чтобы установить сертификат с помощью программы КриптоПро CSP, выполните следующие действия:

- 1 Войдите в Личный кабинет (см. «Вход в Личный кабинет» на стр. 6).
- 2 В списке заявок выберите заявку в статусе **Завершена** и нажмите на ее номер/строчку.

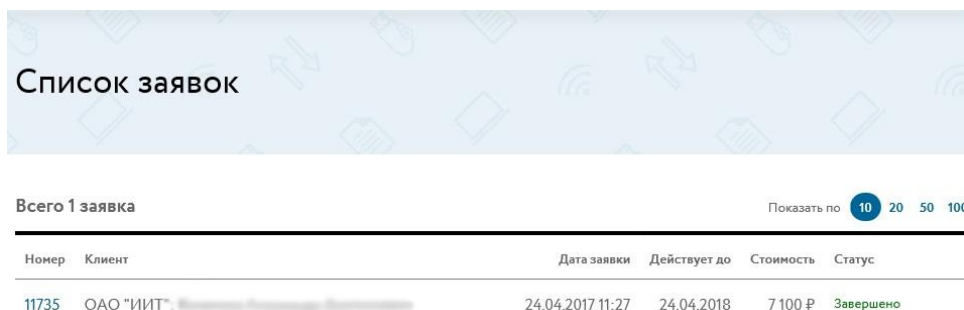


Рисунок 31. Выбор заявки со статусом «Завершено»

- 3 На странице заявки нажмите кнопку **Установить**.



**Внимание!** Далее в этом разделе описано добавление сертификата в контейнер ключей программы КриптоПро CSP. Если вы используете другой криптопровайдер, следуйте подготовленной для него инструкции.

- 4 Введите пароль доступа к контейнеру ключей. Установите флажок **Запомнить пароль**, если не хотите в дальнейшем вводить пароль к этому контейнеру ключей. Нажмите кнопку **ОК**.

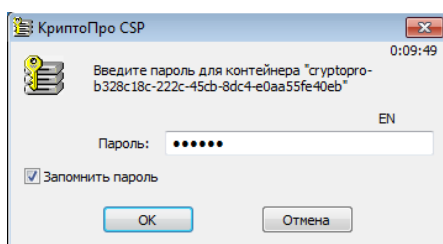


Рисунок 32. Окно ввода пароля к контейнеру ключей программы КриптоПро CSP

- 5 Если Вы ввели верный пароль, то Вы увидите сообщение об успешной установке сертификата.

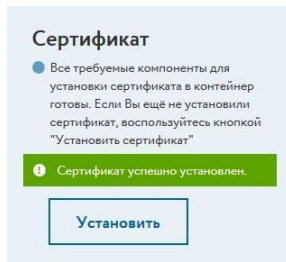


Рисунок 33. Сертификат успешно установлен

# Глоссарий

## Верификация заявки

Проверка запроса на получение услуг удостоверяющего центра (выдачу сертификата), проводимая Агентом. В случае успешной верификации УЦ ИИТ выполняет издание сертификата.

## Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

## Абонент

Клиент организации. Иными словами, это лицо, которое обращается в удостоверяющий центр для получения услуги выпуска сертификата.

## Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

## Агент

Организация-партнер удостоверяющего центра ИИТ, который занимается верификацией запросов на выпуск сертификатов, завершением заявок и выдачей сертификатов.

## Токен

Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т. д. Как правило, это физическое устройство, используемое для упрощения аутентификации.

## Точка выдачи

Физическое месторасположение организации, выполняющей роль удостоверяющего центра, ответственные сотрудники которой выполняют верификацию заявок.

## Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

## Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, который позволяет инициализировать датчик случайных чисел на основе действий пользователя.