# uTrust.User

## Руководство пользователя

ИНФОТЕКС
ТРАСТ

# Содержание

# Введение

## Для кого предназначен документ

Данное руководство предназначено для пользователей программы для ЭВМ uTrust.User (далее – uTrust.User, личный кабинет, программное обеспечение), правообладателем которой является акционерное общество «Инфотекс Интернет Траст». В нем содержится подробная информация о функциональном назначении и возможностях использования программного обеспечения, а также о процедурах подачи заявок, генерации запроса на сертификат и установки сертификата на рабочее место.

# О программном обеспечении uTrust.User

## Назначение программного обеспечения uTrust.User

Программное обеспечение uTrust.User (далее - личный кабинет) — это ваш индивидуальный сервис с веб-интерфейсом для быстрого и удобного получения услуг удостоверяющего центра «Инфотекс Интернет Траст». Для получения сертификата ключа электронной подписи необходимо сначала создать заявку на получение услуг удостоверяющего центра (далее — УЦ), в которой передаётся информация о пользователе, а затем — создать запрос на сертификат.

## Жизненный цикл запроса на сертификат

Основным сценарием работы с личным кабинетом является создание и обработка запроса насертификат (рисунок 1).

**Рисунок 1.** Жизненный цикл запроса на сертификат

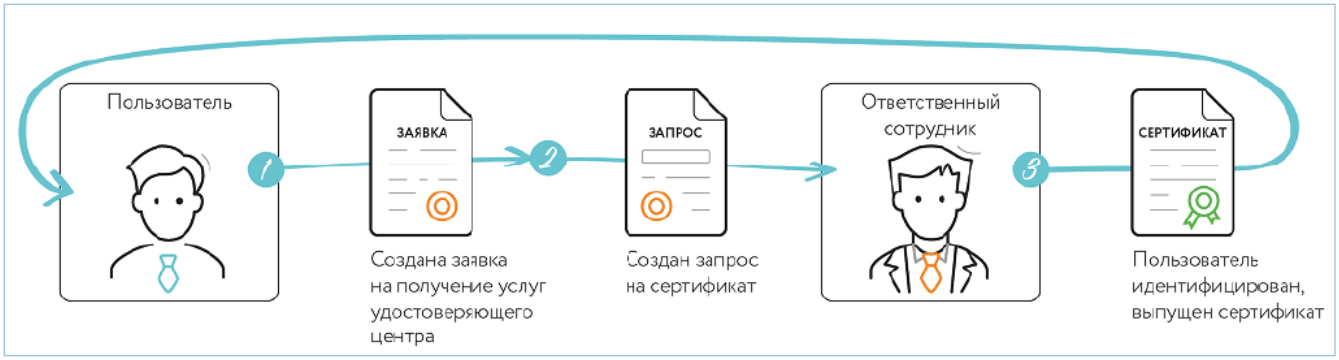


*Рисунок 1. Жизненный цикл запроса на сертификат*

Работа с запросом на сертификат происходит в следующем порядке:

1. Пользователь создаёт заявку на получение услуг удостоверяющего центра.
2. Пользователь в рамках этой заявки создаёт запрос на сертификат.
3. Ответственный сотрудник проводит идентификацию пользователя и издаёт 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;
  - КриптоПро CSP последней доступной версии;
  - JCrypto последней доступной версии;
  - криптопровайдеры, встроенные в токен.
- дополнительное программное обеспечение:
  - JavaLSS;
  - JC-WebClient.

# Обратная связь

Для решения возникающих проблем обратитесь в службу технической поддержки компании «Инфотекс Интернет Траст»:

- электронный адрес службы поддержки: supportIIT@iitrust.ru;
- форма запроса в службу технической поддержки: http://www.iitrust.ru/support/request.php;
- 8 (800) 250-0-265 — «горячая линия» службы технической поддержки (звонок бесплатный для любого региона);
- 8 (800) 250-8-265 — «горячая линия» службы продаж и абонентского обслуживания (звонок бесплатный для любого региона).

# Начало работы с программным обеспечением uTrust.User

## Регистрация в программном обеспечении uTrust.User

Для начала работы с uTust.User вам не нужно проходить отдельную процедуру регистрации. Если у вас ещё нет учётной записи для входа в uTust.User, то она будет создана автоматически в процессе создания заявки на получение услуг УЦ (см. Создание заявки на получение услуг удостоверяющего центра).

## Вход в программное обеспечение uTrust.User

Чтобы просмотреть свои заявки и создать запрос на сертификат (см. Создание запроса на сертификат ), предварительно войдите в личный кабинет. Для этого выполните следующие действия:

1 Откройте веб-сайт личного кабинета. Для этого перейдите по ссылке, полученной у вашего персонального менеджера (см. глоссарий).

2 Нажмите «Войти». Откроется страница входа.

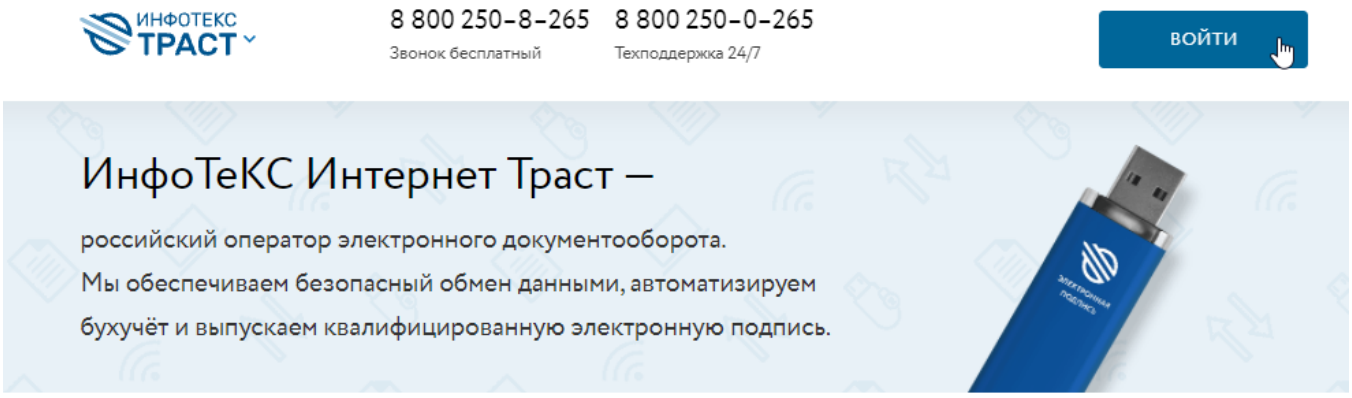


*Рисунок 2. Просмотр страницы входа в личный кабинет*

3 В соответствующих полях введите логин и пароль от личного кабинета. Если вы ещё не зарегистрированы, выберите услугу, подайте заявку и вам автоматически будет создан ваш личный кабинет.

4 Нажмите кнопку «Войти» (рисунок 3).

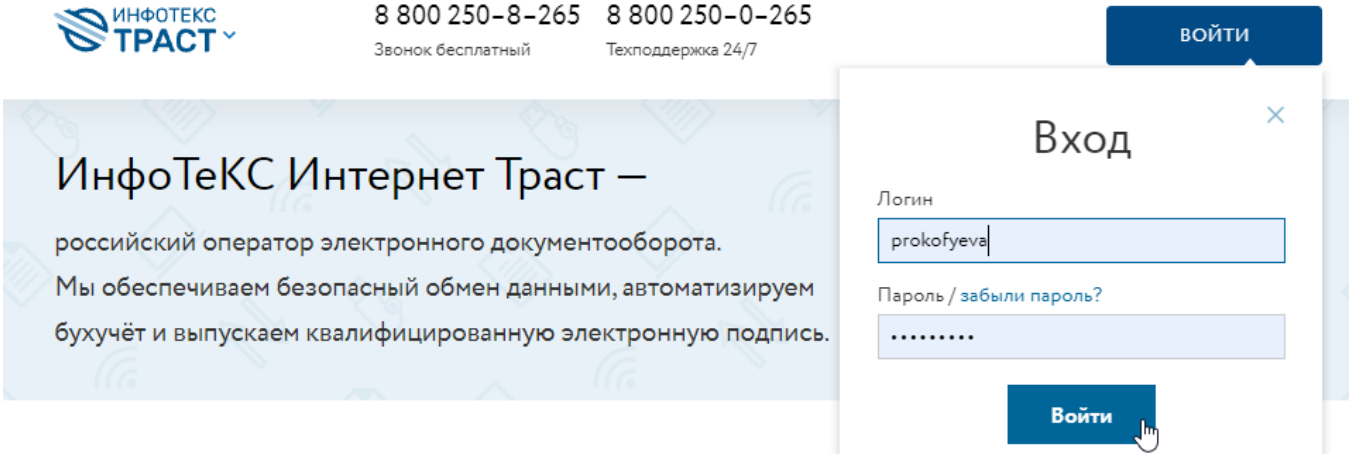


*Рисунок 3. Ввод учётных данных пользователя для входа в личный кабинет*

# Работа в программном обеспечении uTrust.User

## Создание заявки на получение услуг удостоверяющего центра

Для получения сертификата ключа электронной подписи необходимо сначала создать заявку на получение услуг удостоверяющего центра (далее — УЦ), в которой передаётся информация о пользователе, а затем — создать запрос на сертификат. Заявка может быть сформирована лично пользователем, или вместо него сформировать заявку на получение услуг УЦ может ответственный сотрудник. Сгенерировать запрос на сертификат может только пользователь.

В заявке указывается регистрационная информация пользователя:

- фамилия, имя и отчество (если имеется);
- наименование должности;
- наименование организации;
- СНИЛС;
- реквизиты паспорта гражданина РФ.

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

1. Если у вас уже есть учётная запись, войдите в нее. Если учётной записи у вас нет, перейдите по ссылке, полученной у представителя удостоверяющего центра.
2. На главной странице личного кабинета в разделе «Заказать электронную подпись» выберите тип заявки на получение услуг удостоверяющего центра (рисунок 4).

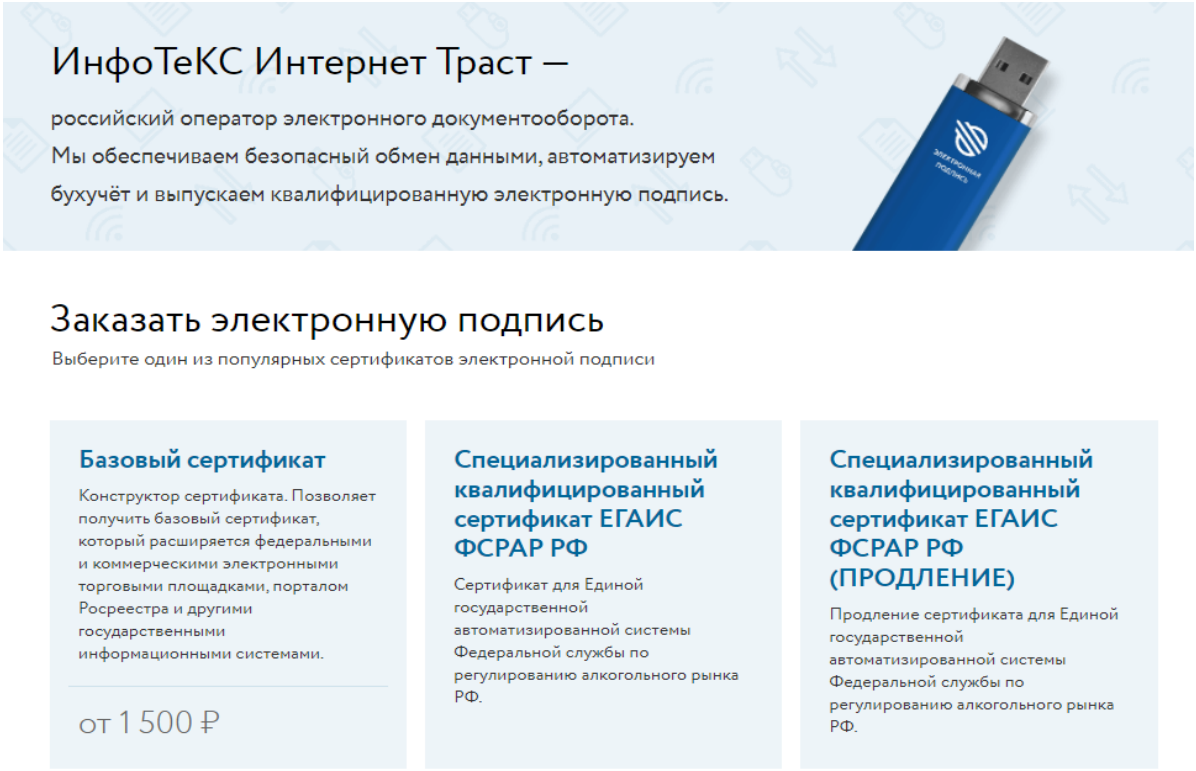


*Рисунок 4. Выбор типа сертификата в разделе «Заказать электронную подпись»*

3 На странице «Сертификат» выберите тип заявителя и необходимые расширения. Нажмите кнопку «Продолжить» (рисунок 5).

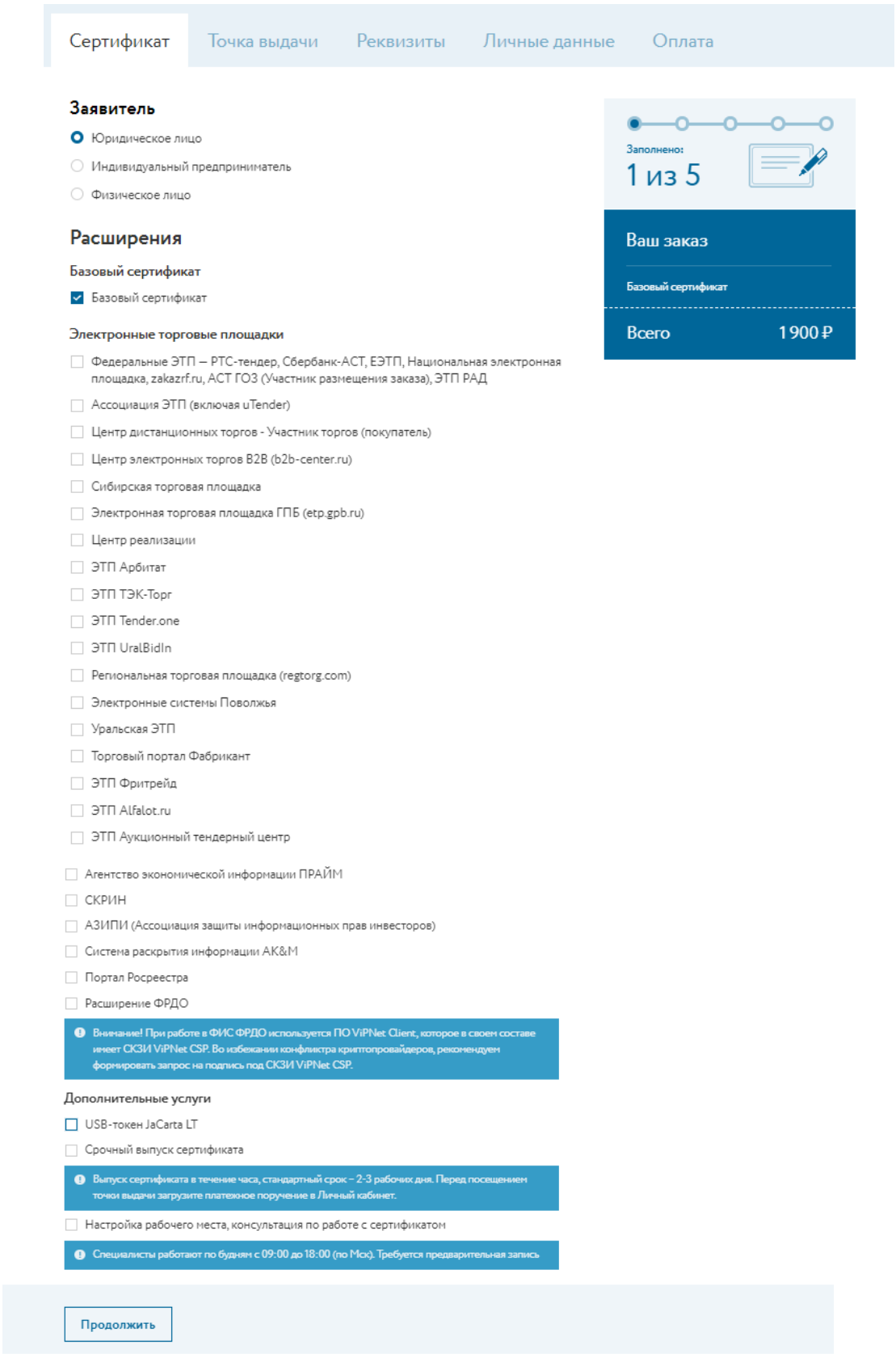


*Рисунок 5. Выбор сфер применения сертификата*

4 На странице «Точка выдачи» просмотрите адрес точки выдачи сертификата (адрес расположения ответственного сотрудника) и нажмите кнопку «Продолжить» (рисунок 6).

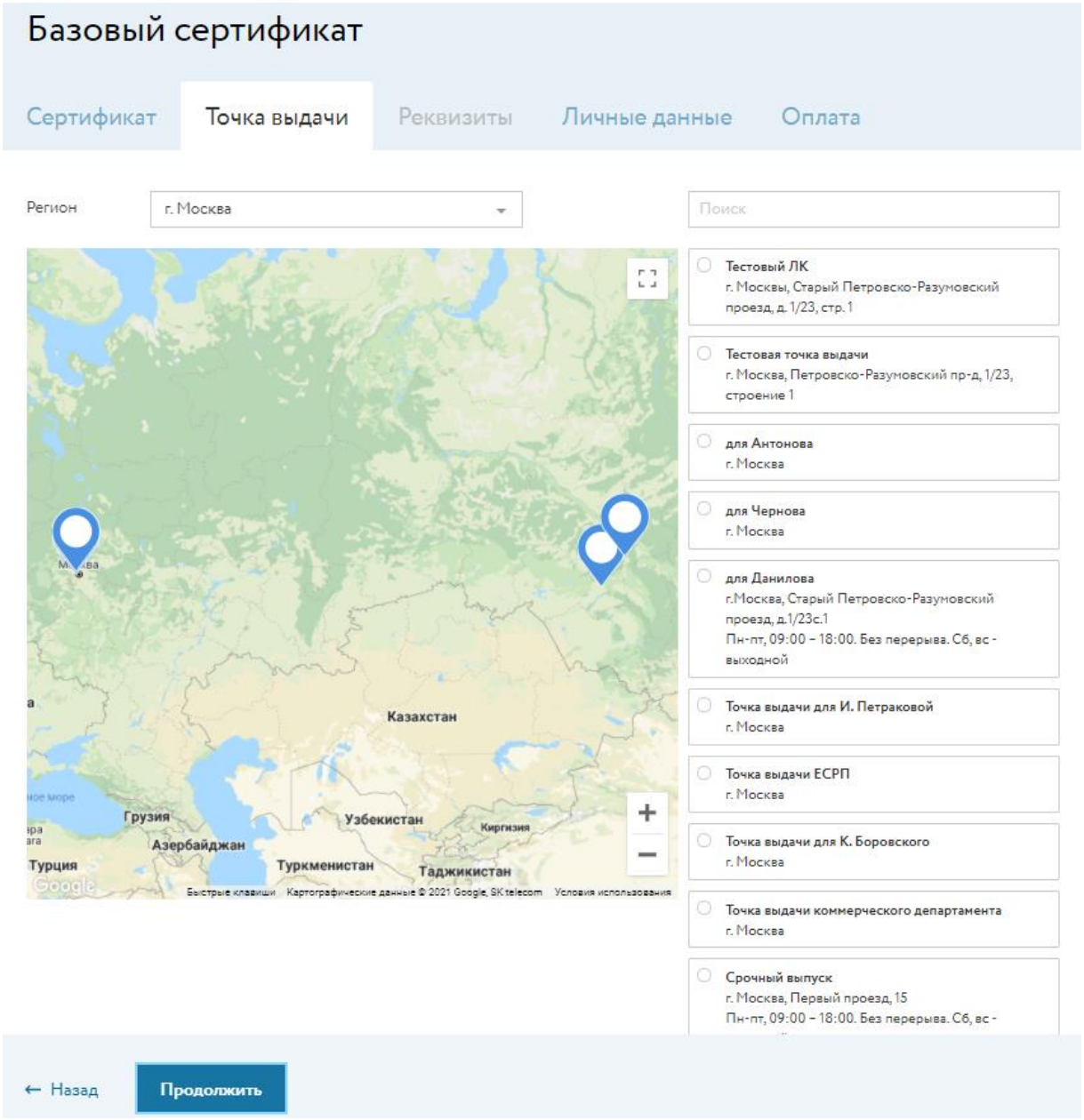


*Рисунок 6. Выбор точки выдачи сертификата*

5 В случае, если заявитель – ЮЛ, на странице «Реквизиты» укажите ИНН (рисунок 7).

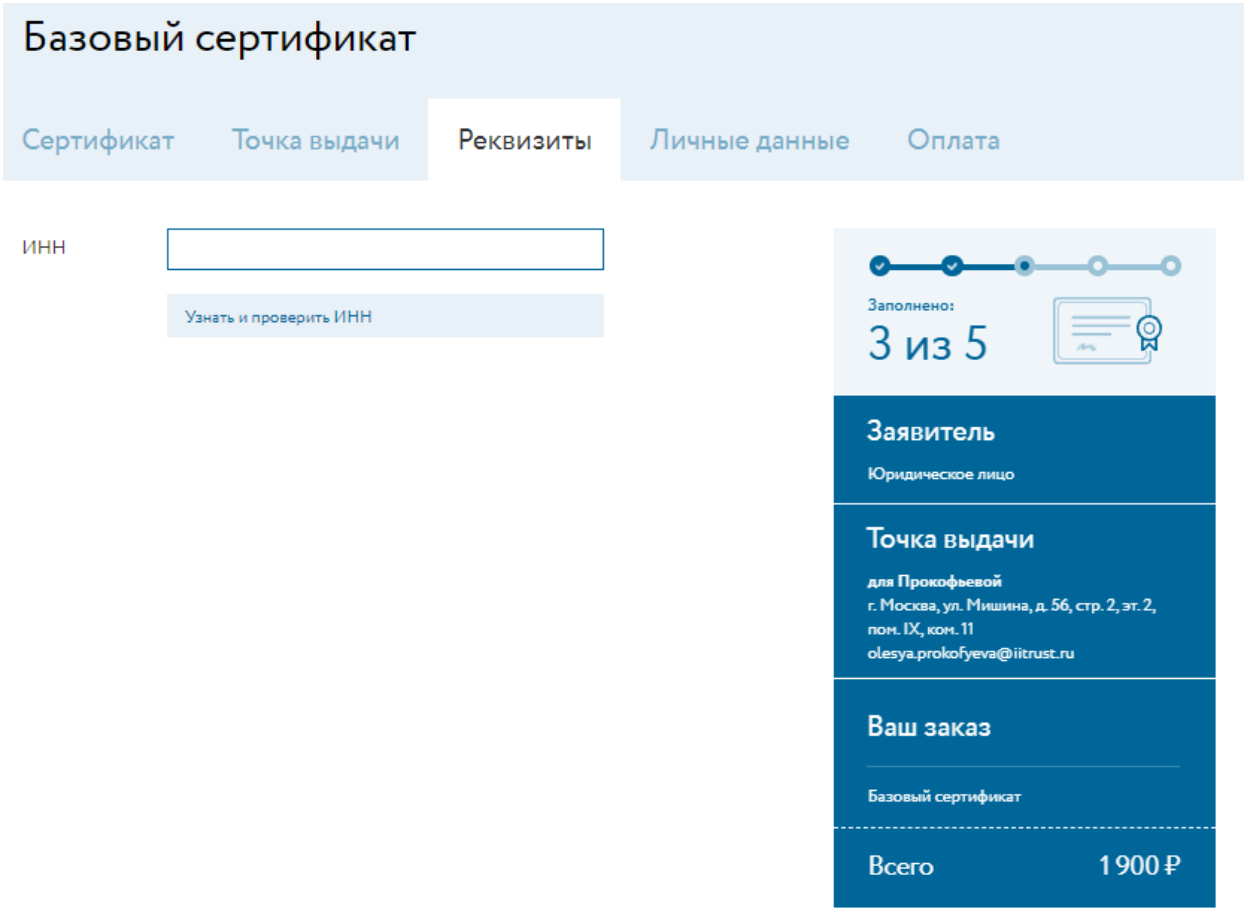


*Рисунок 7. Ввод ИНН*

Реквизиты организации загружаются автоматически по ИНН вашей организации. В соответствующих полях проверьте и отредактируйте реквизиты вашей организации и нажмите кнопку «Продолжить» (рисунок 8).

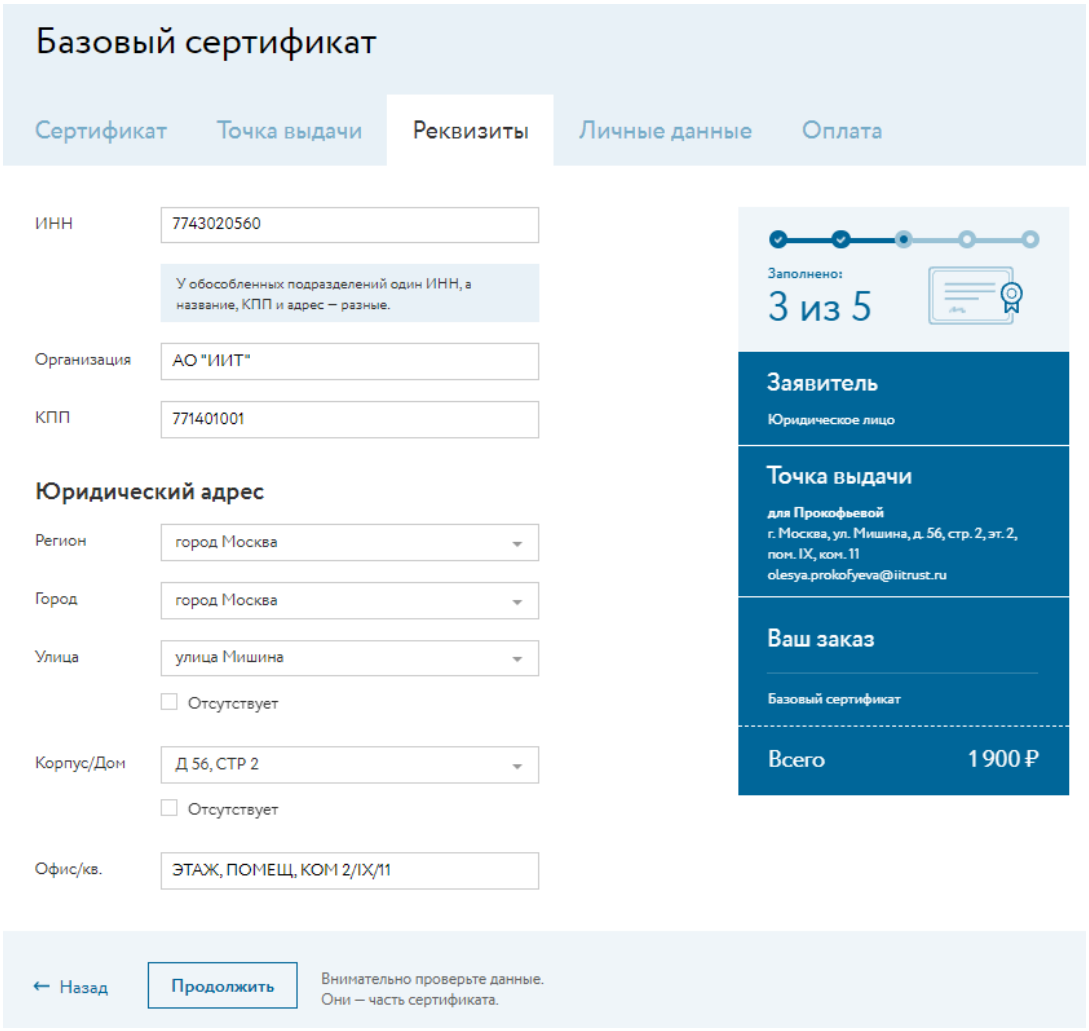


*Рисунок 8. Редактирование реквизитов организации.*

6 На странице «Личные данные» в разделе «Данные владельца сертификата» укажите личные данные пользователя (рисунок 9).

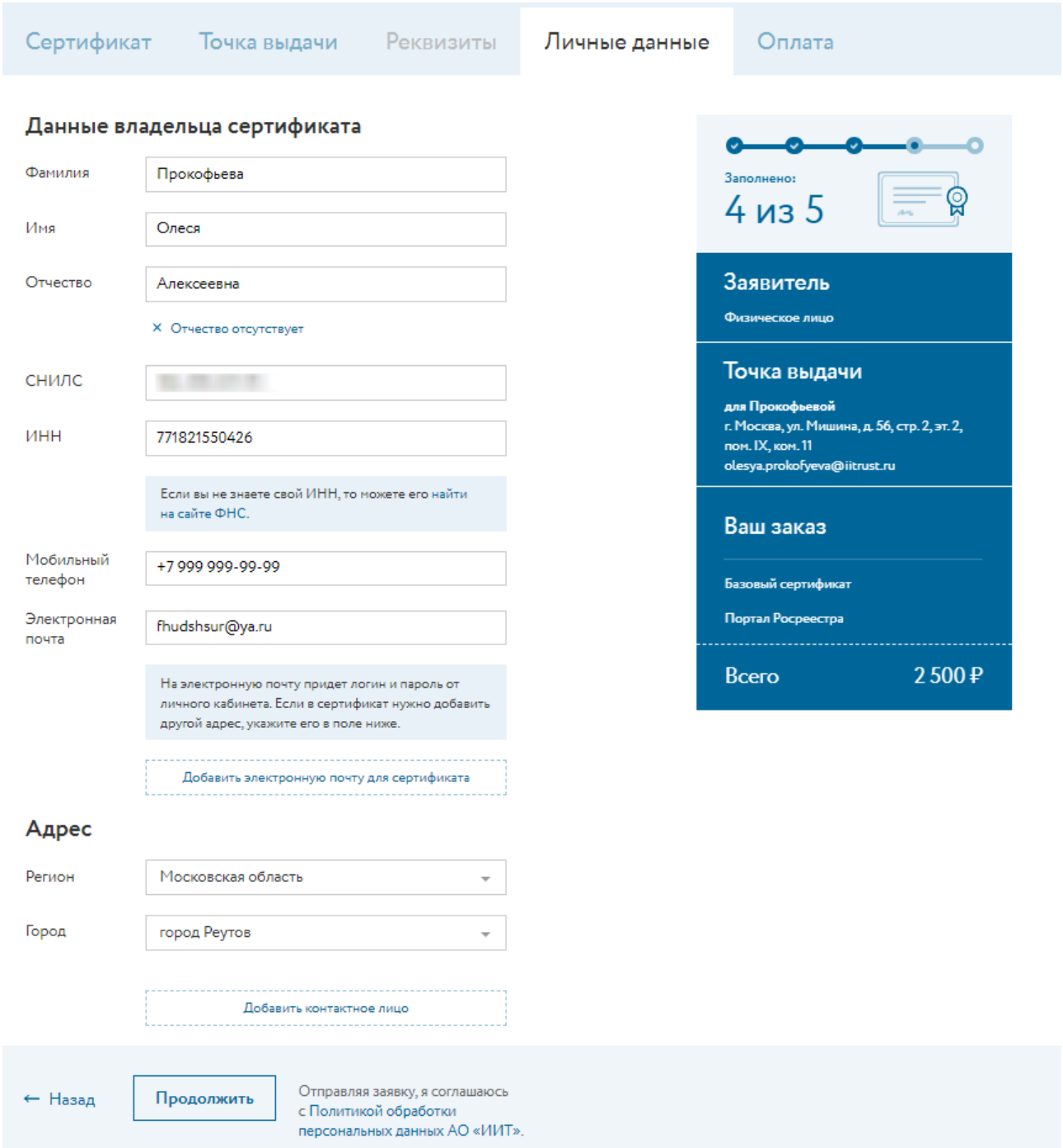


*Рисунок 9. Указание данных о пользователе*

7 На странице «Оплата» выберите форму оплаты. Для ФЛ/ИП — по карте или счёту, для ЮЛ — только по счёту (рисунок 10).

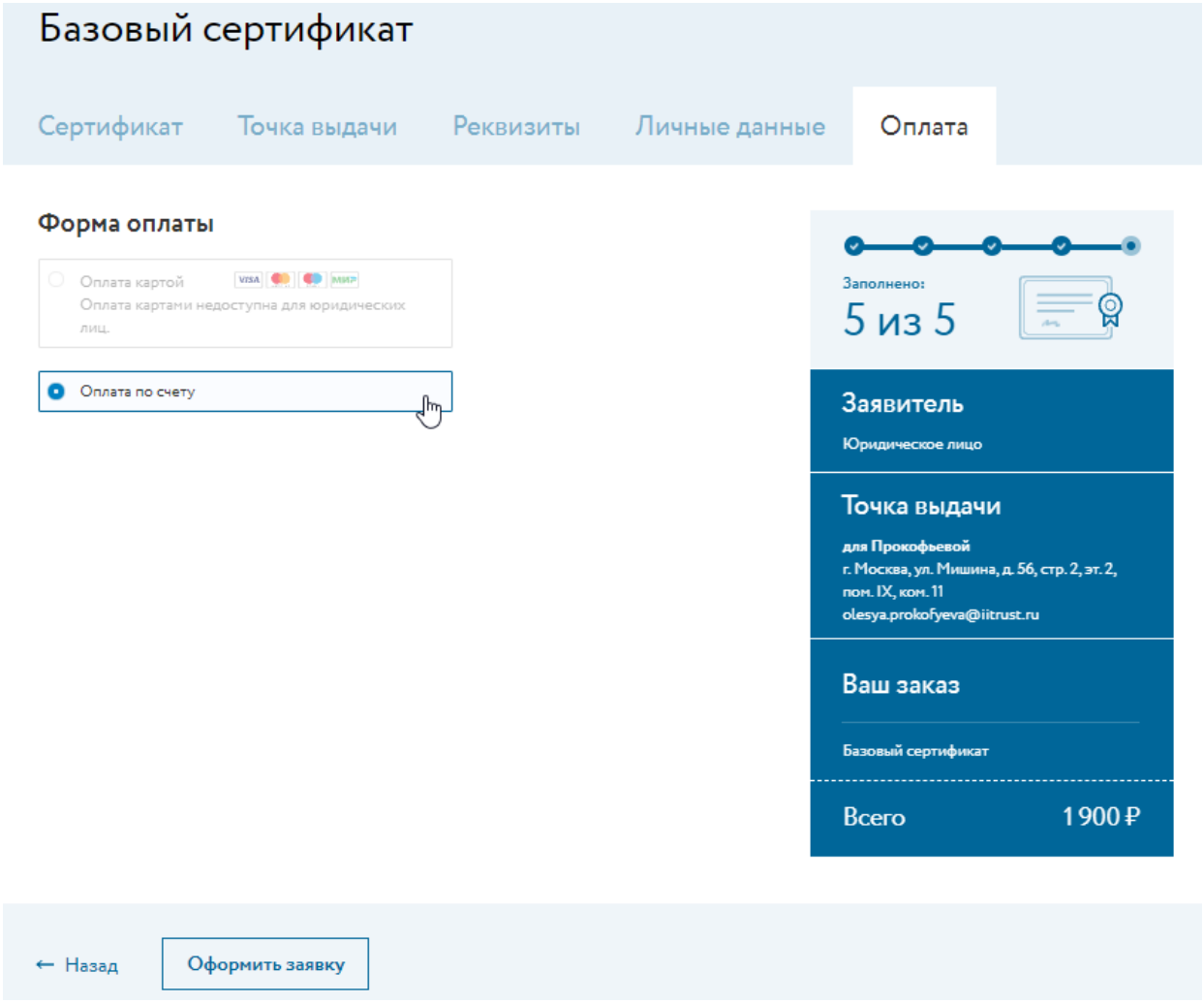


*Рисунок 10. Выбор формы оплаты*

Появится сообщение о том, что заявка успешно оформлена. После создания заявки вы получите по электронной почте письмо с вашими учётными данными для входа в личный кабинет (если вы создавали заявку впервые). Войдите в личный кабинет и создайте запрос на сертификат (см. Создание запроса на сертификат ).

# Создание запроса на сертификат

После того, как Вы создали заявку на получение услуг удостоверяющего центра, вы можете создать запрос на сертификат. В зависимости от установленного на вашем компьютере криптопровайдера следуйте указаниям одного из разделов:

- Создание запроса на сертификат с помощью программы ViPNet CSP
- Создание запроса на сертификат с помощью программы КриптоПро CSP

**Внимание! Генерировать запрос можно:**

1. **На компьютер, на котором будет происходить дальнейшая работа с сертификатом.**
2. **На токен (при использовании токена не забудьте подключить его к компьютеру).**

## Создание запроса на сертифика с помощью программы ViPNet CSP

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

1 Войдите в Личный кабинет (см. Вход в программное обеспечение uTrust.User).

2 После входа в личный кабинет вы увидите список ваших заявок. Щёлкните номер заявки в статусе «Ожидание запроса на сертификат» (рисунок 11).

| Номер | Клиент | Дата подачи | Точка выдачи | Стоимость | Статус | Сертификат |
|---|---|---|---|---|---|---|
| 4296 | АО "ИИТ": Пркоофьева Олеся Алексеевна | 12.10.2021 | 77 - для Прокофьевой | 1900 Оплачено | Ожидание запроса на сертификат | |

*Рисунок 11. Просмотр списка заявок*

3 Откроется страница просмотра заявки. если на панель «Процесс» вы видите сообщение о необходимости установки дополнительного программного обеспечения, выполните его установку, перейдя по ссылке (рисунок 12).


*Рисунок 12. Просмотр сообщения о необходимости установки дополнительного программного обеспечения*

4 На панели «Процесс» нажмите кнопку «Сгенерировать запрос» (рисунок 13).

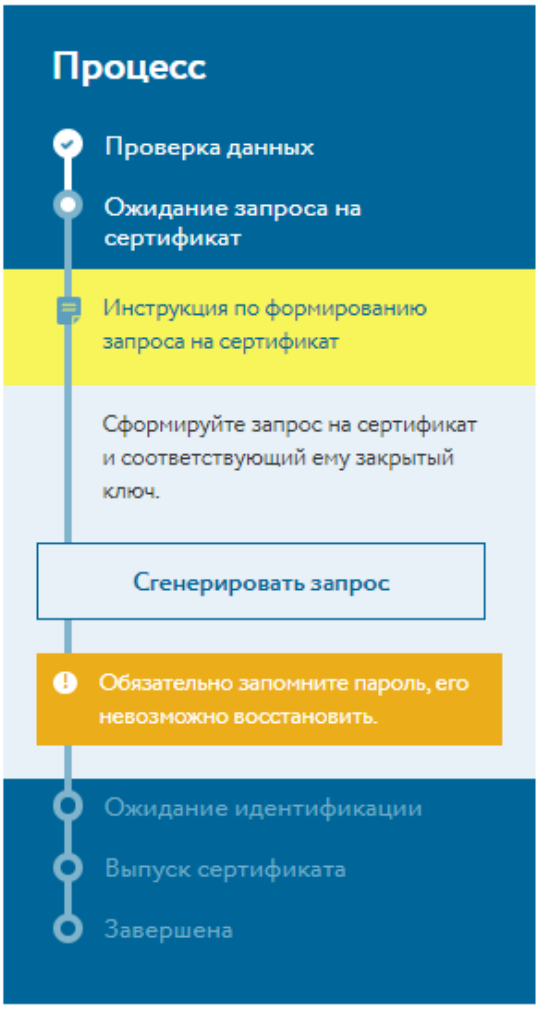


*Рисунок 13. Создание запроса на сертификат*

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

5 В окне «Создание ключа электронной подписи» в списке «Использовать криптопровайдер»

выберите Infotecs Cryptographic Service Provider и нажмите кнопку «Создать ключ электронной подписи» (рисунок 14).

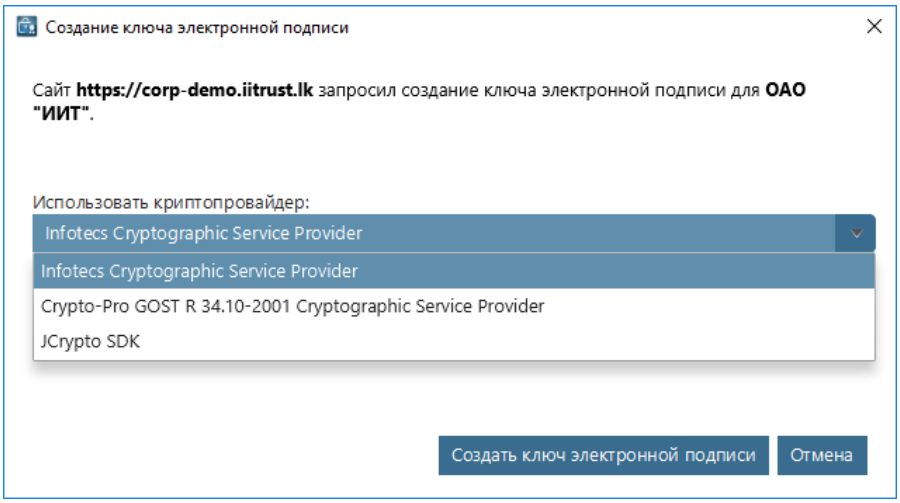


*Рисунок 14. Выбор криптопровайдера*

6 В появившемся окне «ViPNet CSP — инициализация контейнера ключей» укажите следующее:

— имя контейнера ключей (или оставьте значение по умолчанию в соответствующем поле);

— место размещения контейнера ключей, установив переключатель в одно из значений: «Папка на диске» или «Выберите устройство».

В зависимости от места размещения контейнера ключей в запрос будет добавлено расширение со следующей информацией:

— при размещении контейнера ключей в папке на диске — с информацией о том, что желаемый срок действия закрытого ключа — 1 год;

— при размещении контейнера ключей на устройстве с аппаратной поддержкой алгоритмов ГОСТ — с информацией о том, что желаемый срок действия закрытого ключа — 3 года.

Нажмите кнопку OK (рисунок 15).

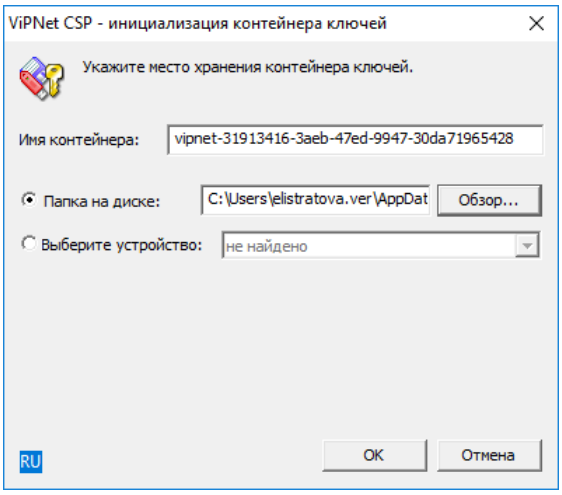


*Рисунок 15. Выбор места хранения контейнера ключей.*

**7** В окне ViPNet CSP — пароль контейнера ключей задайте пароль доступа к контейнеру ключей.

---

Внимание! Обязательно запомните пароль, восстановить его нельзя. Если вы потеряете пароль, необходимо будет создавать новую заявку.

---

Установите флажок «Сохранить пароль», если не хотите в дальнейшем вводить пароль к этому контейнеру ключей и нажмите кнопку OK (рисунок 16).

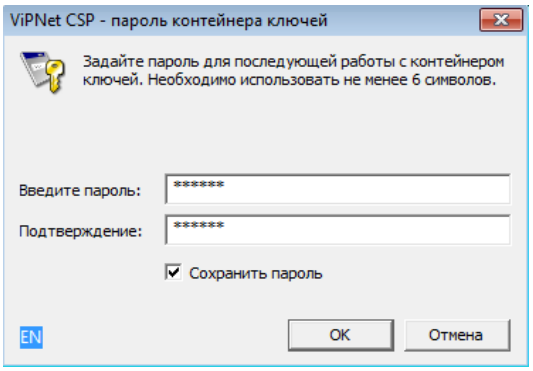


*Рисунок 16. Создание пароля контейнера ключей*

**8** Появится электронная рулетка. Поводите указателем в пределах окна «Электронная рулетка» (рисунок 17).

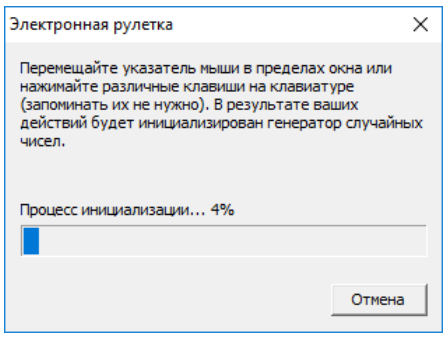


*Рисунок 17. Просмотр окна «Электронная рулетка»*

**9** Если при создании пароля доступа к контейнеру ключей вы не установили флажок «Сохранить пароль», в следующем окне введите пароль. Нажмите кнопку ОК.

**10** Ваша заявка получит статус «Ожидание идентификации» (рисунок 18).

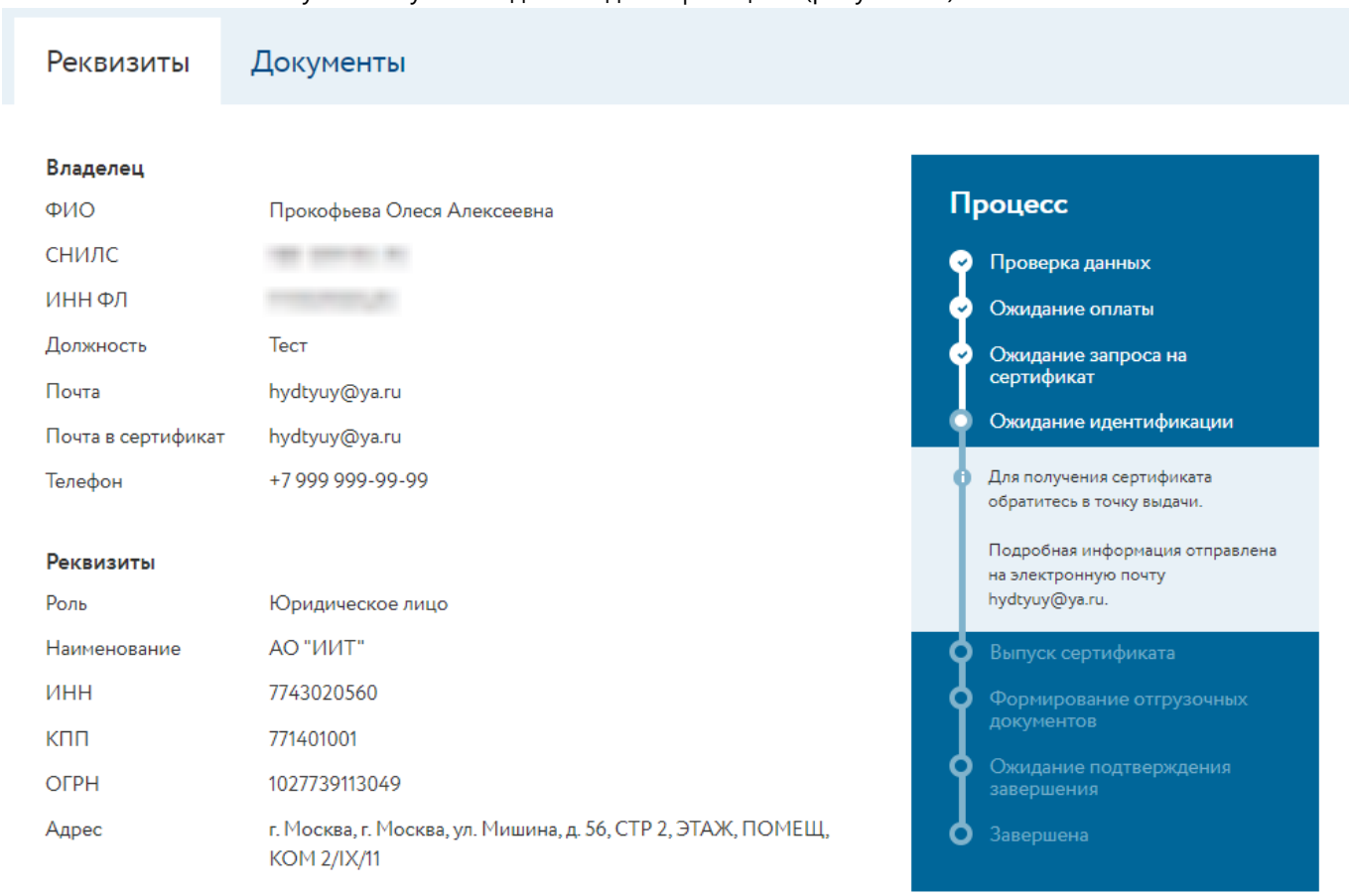


*Рисунок 18. Ожидание идентификации*

Для прохождения идентификации и получения сертификата обратитесь в точку выдачи, которую вы выбрали ранее. Для прохождения идентификации вам понадобится предоставить сотруднику необходимые документы, а также расписаться в предоставленном сотрудником бланке сертификата. Как только вы пройдёте идентификацию у ответственного сотрудника, сертификат будет издан, и вы сможете установить его.

# Создание запроса на сертификат с помощью программы КриптоПро CSP

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

1. Войдите в личный кабинет (см. Вход в программное обеспечение uTrust.User).
2. После входа в личный кабинет вы увидите список ваших заявок. Щёлкните номер заявки в статусе «Ожидание запроса на сертификат» (рисунок 19).

| Номер | Клиент | Дата подачи | Точка выдачи | Стоимость | Статус | Сертификат |
|---|---|---|---|---|---|---|
| 4296 | АО "ИИТ": Пркоофьева Олеся Алексеевна | 12.10.2021 | 77 - для Прокофьевой | 1900 Оплачено | Ожидание запроса на сертификат | |

*Рисунок 19. Просмотр списка заявок*

3. Откроется страница просмотра заявки. Если на панели «Процесс» вы видите сообщение о необходимости установки дополнительногоо программного обеспечения, выполните его установку (рисунок 20).


*Рисунок 20. Просмотр сообщения о необходимости установки дополнительного программного обеспечения*

4. На панели «Процесс» нажмите кнопку «Сгенерировать запрос» (рисунок 21).

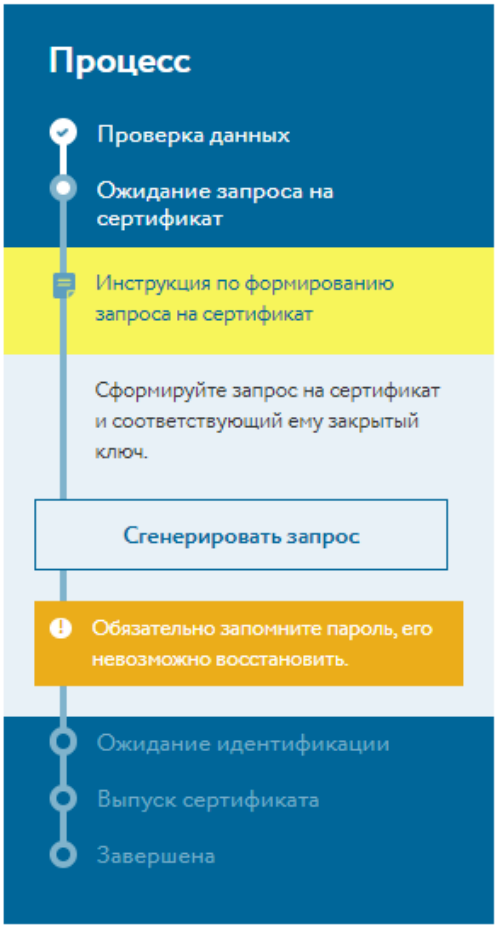


*Рисунок 21. Создание запроса на сертификат*

---

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

---

**5** В окне «Создание ключа электронной подписи» в списке «Использовать криптопровайдер» выберите Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider и нажмите кнопку «Создать ключ электронной подписи» (рисунок 22).

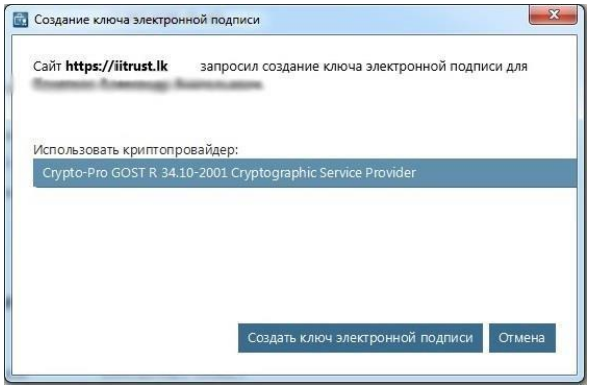

*Рисунок 22. Выбор криптопровайдера для создания ключа электронной подписи*

6 В появившемся окне КриптоПро CSP выберите носитель для хранения контейнера ключей и нажмите кнопку «OK» (рисунок 23).

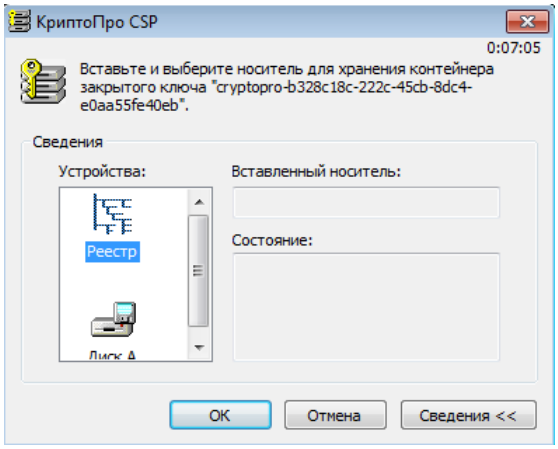


*Рисунок 23. Выбор места хранения контейнера ключей*

7 Появится электронная рулетка. Поводите указателем в пределах окна электронной рулетки (рисунок 24).

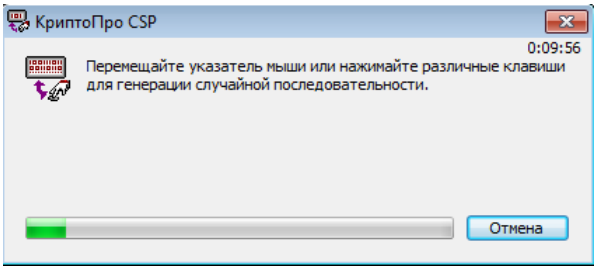


*Рисунок 24. Просмотр окна «Электронная рулетка»*

8 В окне КриптоПро CSP задайте пароль доступа к контейнеру ключей и подтвердите его. Нажмите кнопку «OK» (рисунок 25).

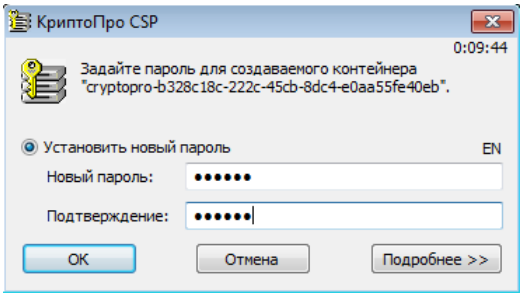


*Рисунок 25. Установка пароля доступа к контейнеру ключей*

9 Введите пароль доступа к контейнеру ключей. Установите флажок «Запомнить пароль», если не хотите в дальнейшем вводить пароль к этому контейнеру ключей. Нажмите кнопку «OK» (рисунок 26).

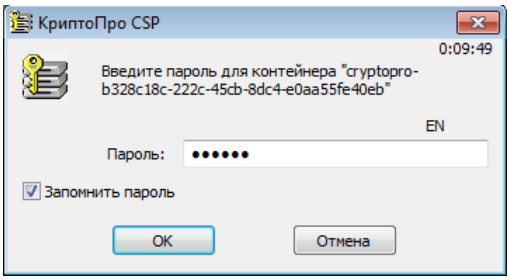


*Рисунок 26. Ввод пароля для контейнера ключей*

**10** Ваша заявка получит статус «Ожидание идентификации» (рисунок 27).

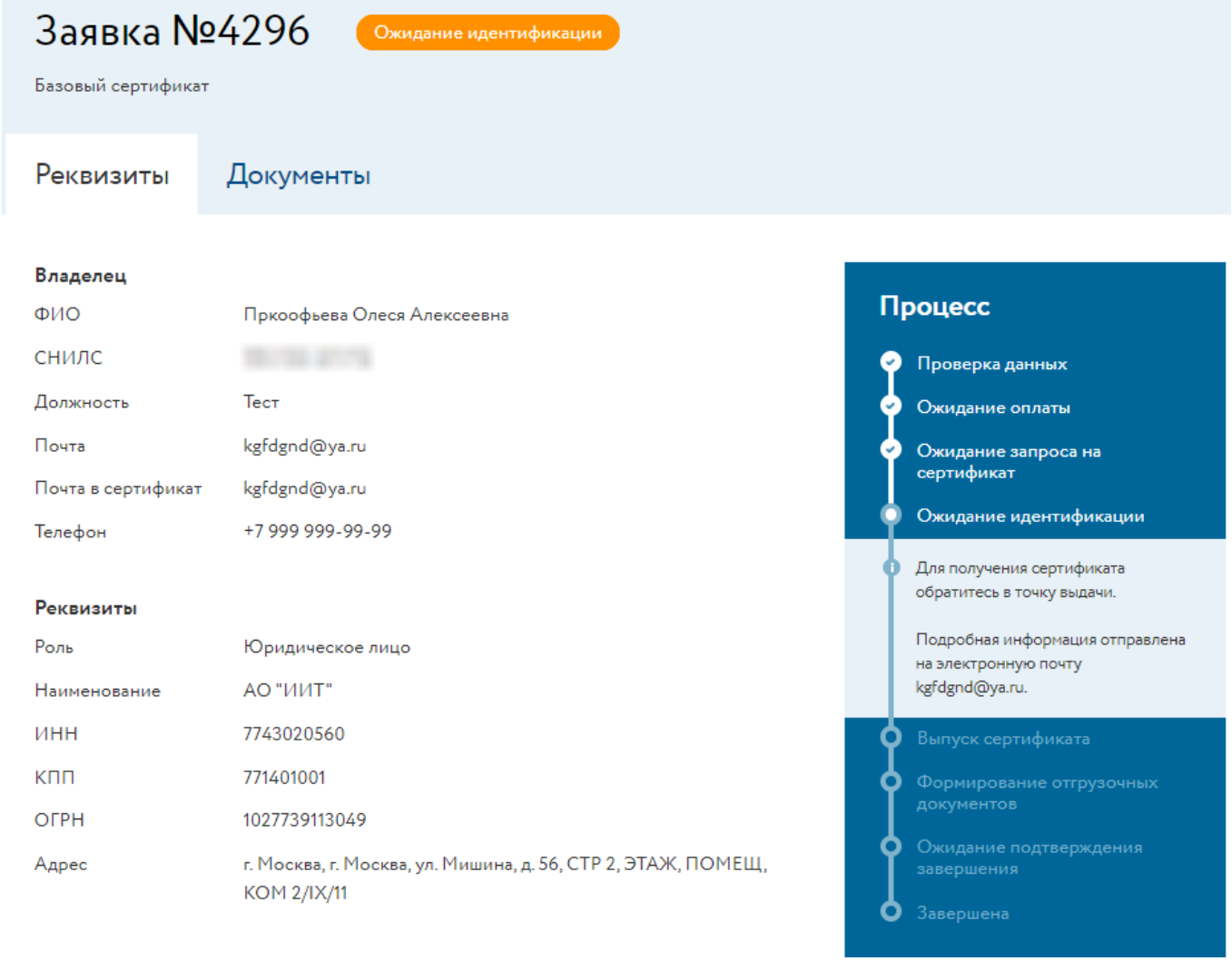


*Рисунок 27. Ожидание идентификации*

**11** Как только вы пройдете идентификацию у ответственного сотрудника,сертификат будет издан и вы сможете установить его (см. Установка сертификата ).

# Установка сертификата

После того, как по вашему запросу (см. Создание запроса на сертификат) будет издан сертификат, вы сможете установить его. Чтобы установить сертификат с помощью вашего криптопровайдера, выполните следующие действия:

1 Войдите в Личный кабинет (см. Вход в программное обеспечение uTrust.User).

2 В списке заявок выберите заявку в статусе «Завершена» и щёлкните на неё (рисунок 28).

| Номер | Клиент | Дата подачи | Точка выдачи | Стоимость | Статус | Сертификат |
|---|---|---|---|---|---|---|
| 4283 | АО "ИИТ": Прокофьева Олеся Алексеевна | 04.10.2021 | 77 - Точка выдачи Корпоративного сценария | Не требует оплаты | Завершена | с 05.10.2021 |

*Рисунок 28. Просмотр списка заявок*

3 На панели «Процесс» нажмите кнопку «Установить» (рисунок 29).

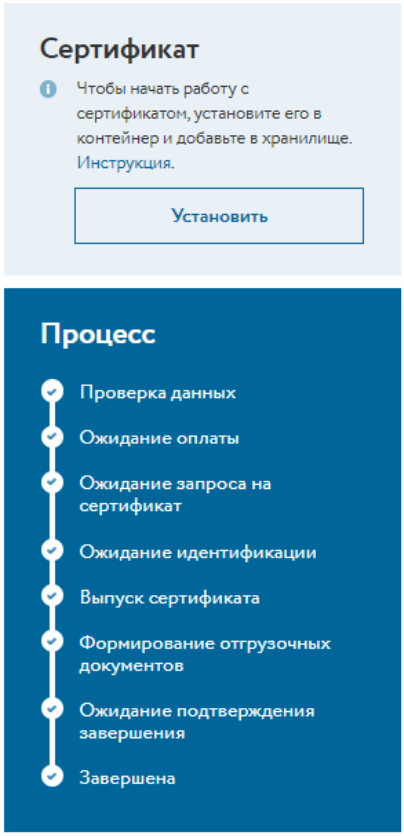


*Рисунок 29. Установка сертификата*

4 В открывшемся окне введите пароль доступа к контейнеру ключей. Если при создании паролядоступа к контейнеру ключей вы не сохраняли пароль, то в зависимости от установленного навашем компьютере криптопровайдера выполните следующее:

— в окне криптопровайдера ViPNet CSP установите флажок «Сохранить пароль» и нажмите кнопку «ОК» (рисунок 30).

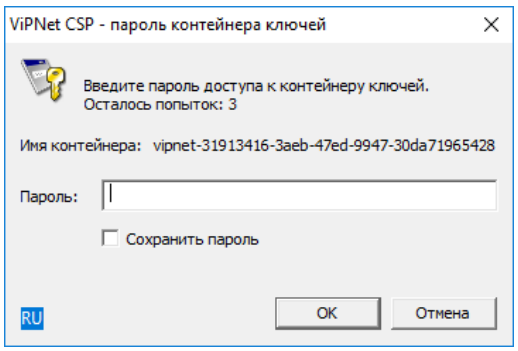


*Рисунок 30. Ввод пароля доступа к контейнеру ключей*

— в окне криптопровайдера КриптоПро CSP установите флажок «Запомнить пароль» инажмите кнопку «OK» (рисунок 31).

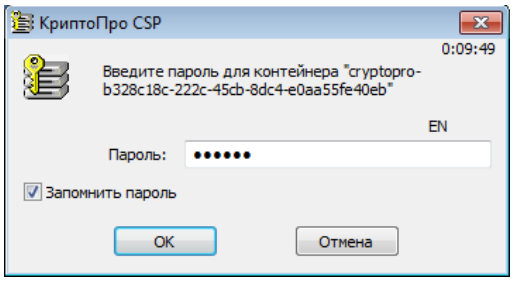


*Рисунок 31. Ввод пароля для контейнера ключей*

Если вы ввели верный пароль, то вы увидите сообщение об успешной установке сертификата (рисунок 32).

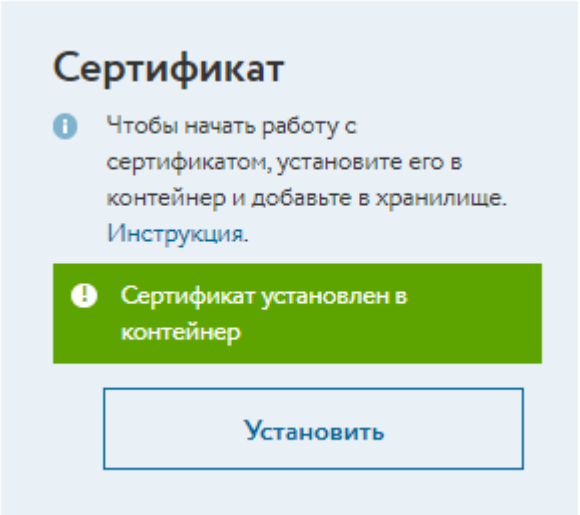


*Рисунок 32. Просмотр сообщения «Сертификат успешно установлен»*

# Глоссарий

## Запрос на сертификат

Защищённое 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).

## Идентификация пользователя

Идентификация, проводимая при личном присутствии пользователя, включающая в себя установление личности владельца сертификата (пользователя) по основному документу, удостоверяющему личность.

## Пользователь

Лицо, присоединившееся к регламенту оказания удостоверяющим центром акционерного общества «Инфотекс Интернет Траст» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, и зарегистрированное в информационной системе удостоверяющего центра.

## Менеджер удостоверяющего центра

Сотрудник удостоверяющего центра, который регистрирует организацию в информационной системе удостоверяющего центра.

## Токен

Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя. Также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и других задач.

## Удостоверяющий центр

Акционерное общество «Инфотекс Интернет Траст», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».