

Инструкция «Порядок заказа сертификатов для пользователей систем электронного документооборота»

Содержание:

Глава 1 Начало работы.

Описаны настройки браузера и порядок работы с сайтом Удостоверяющего Центра ООО «Кейсистемс».

Глава 2 Подготовка документов.

Приведен список документов для прохождения регистрации пользователя и их формы для самостоятельного заполнения.

Глава 3 Регистрации нового пользователя.

Описана процедура регистрации пользователя на сайте Удостоверяющего Центра ООО «Кейсистемс».

Глава 4 Формирование запроса на сертификат.

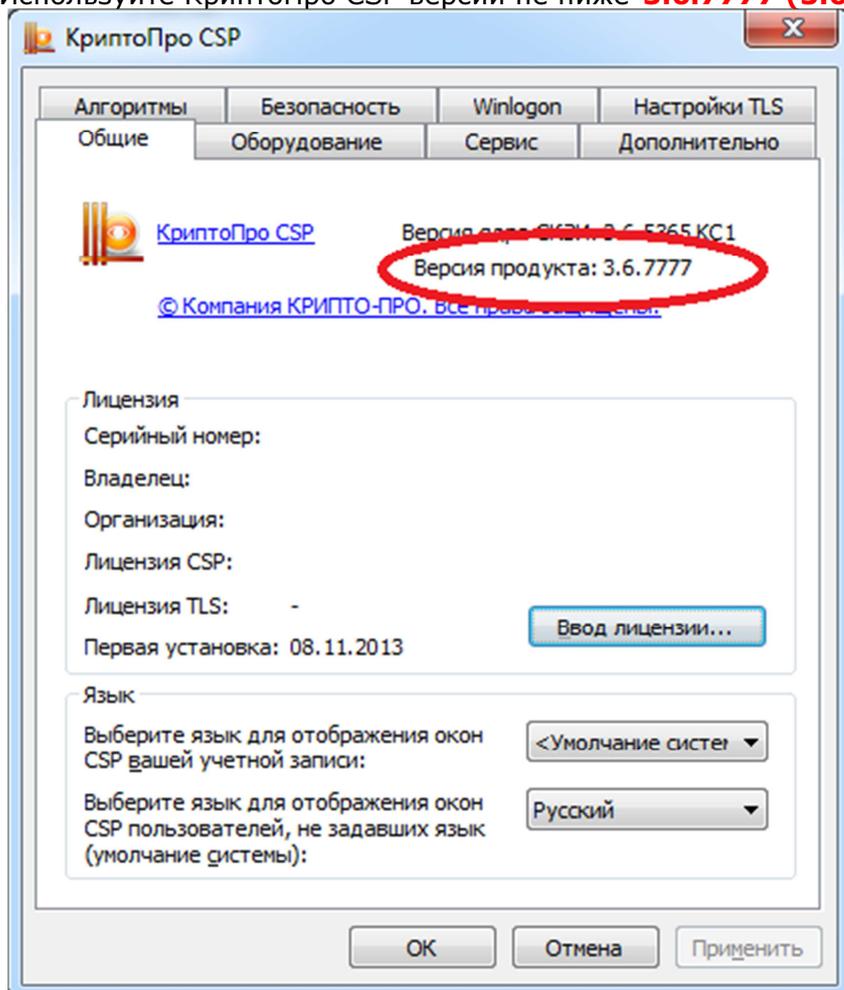
Получение сертификата.

Описана процедура формирования запроса на сертификат, печати бланка запроса на сертификат, сохранения и установки сертификата.

Глава 1 Начало работы

Перед началом работы проверьте версии используемого программного обеспечения:

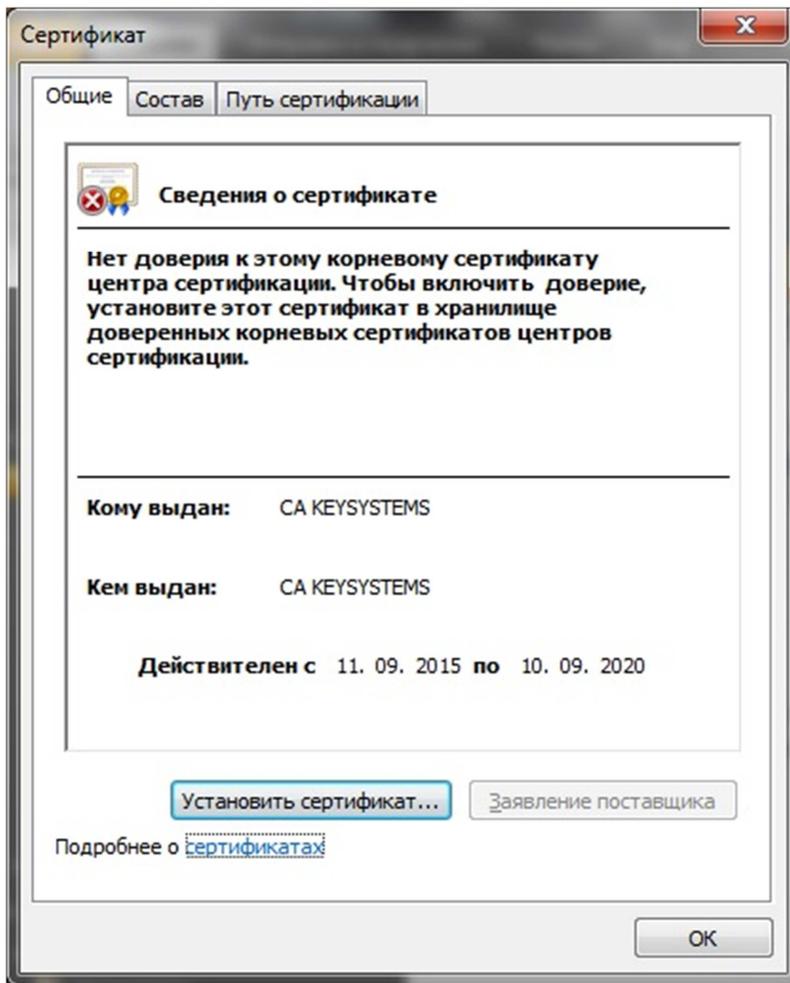
- 1) Используйте только INTERNET EXPLORER версий **8,9 или 10**
- 2) Используйте КриптоПро CSP версии не ниже **3.6.7777 (3.6 R4)**:



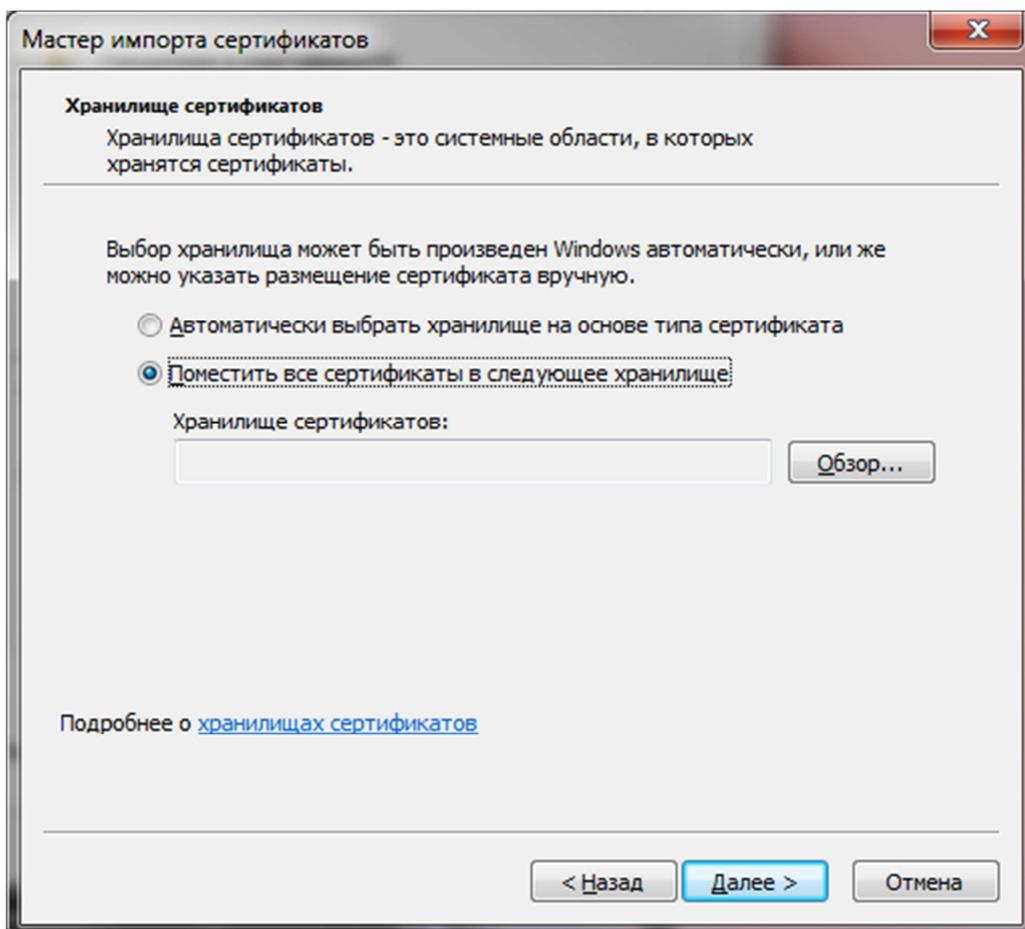
Скачать Крипто-Про CSP можно по ссылке:

http://keysystems.ru/files/CA/DISTR/CryptoPro_CSP/cspsetup.exe

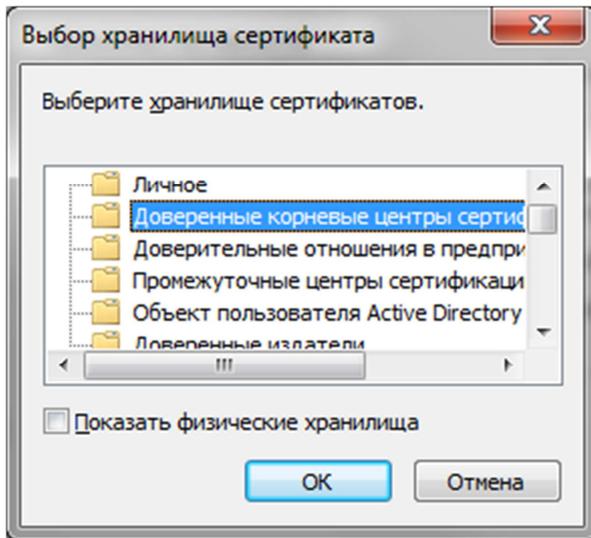
- 3) Установите драйвер для Рутокен  или E-token .
- Драйвер Рутокен: <http://keysystems.ru/files/CA/DISTR/Rutoken/>
- Драйвер E-token: <http://keysystems.ru/files/CA/DISTR/E-token/>
- 4) Скачайте по ссылке <http://keysystems.ru/files/CA/DISTR/cakeysystems2015.cer> и установите корневой сертификат в хранилище «доверенные корневые центры сертификации».



Нажмите кнопку «Установить сертификат» - Далее - Поместить все сертификаты в следующее хранилище - Обзор

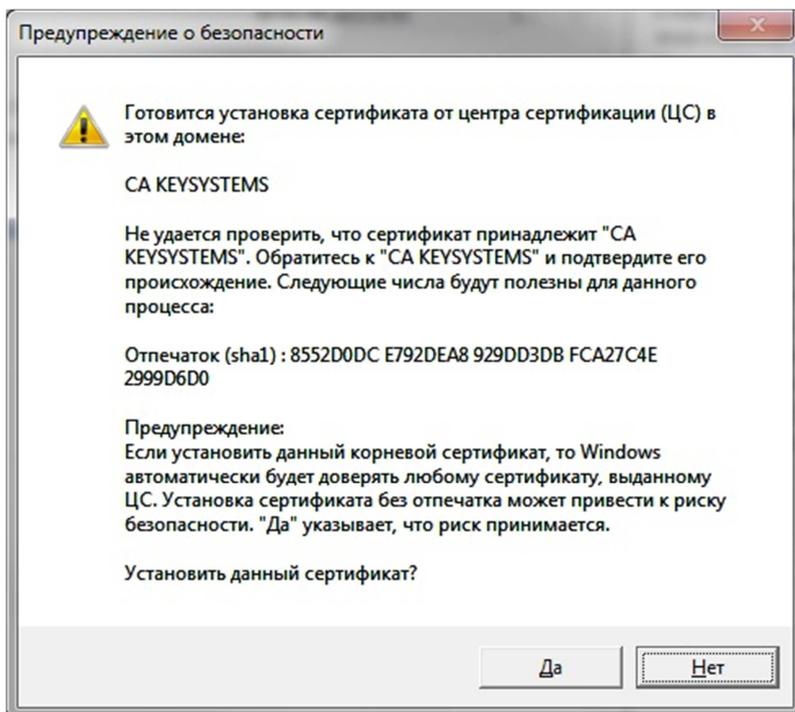


Доверенные корневые центры сертификации – ОК

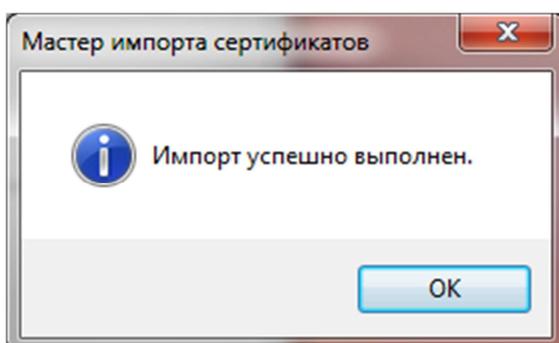


Далее - Готово

Появится окно «Предупреждение о безопасности». Нажмите «Да»

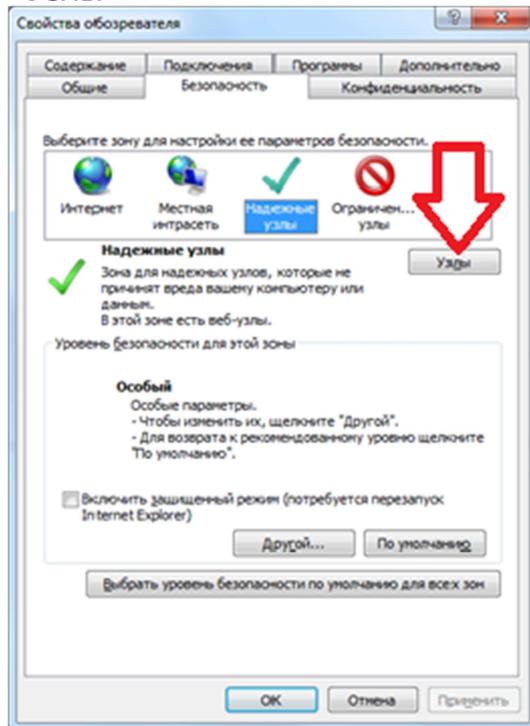


Если появилось такое окно, значит корневой сертификат успешно установлен:



Добавьте веб-узел <https://ra.keysystems.ru/ui/> в надежные узлы Internet Explorer:

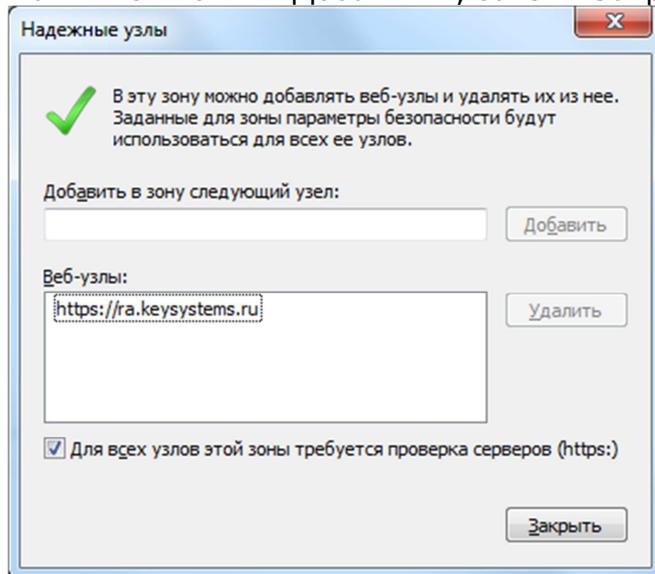
Откройте «Свойства обозревателя» – закладка «Безопасность» - кнопка «Узлы»



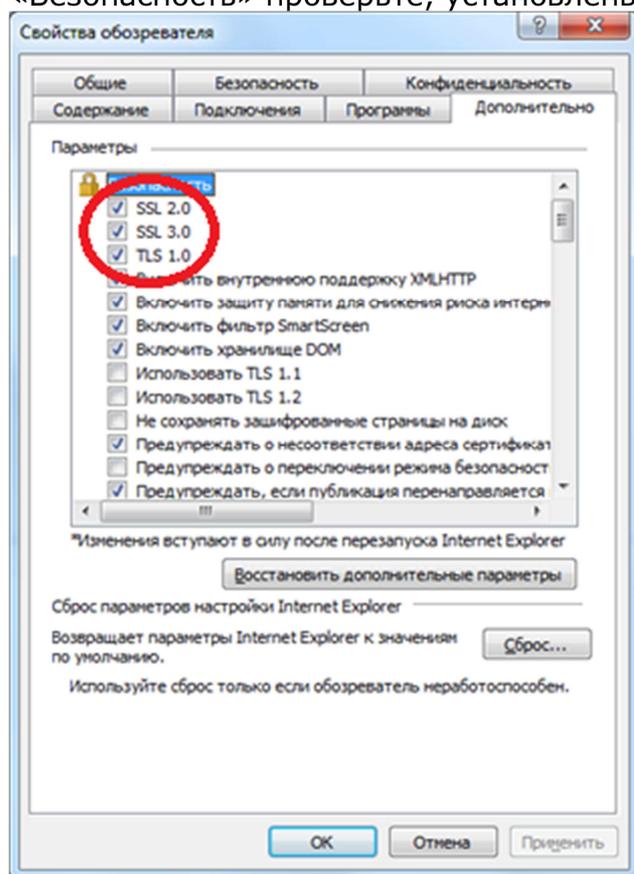
В поле «Добавить в зону следующий узел» введите

<https://ra.keysystems.ru>

Нажмите кнопки «Добавить», затем «Заккрыть»



В окне «Свойства обозревателя» на закладке «Дополнительно» в разделе «Безопасность» проверьте, установлены ли ВСЕ галочки.



Глава 2 Подготовка документов

Заполните следующие документы:

Заявление о присоединении к Регламенту Удостоверяющего Центра
(Приложение № 1 к Регламенту УЦ ООО «Кейсистемс»)

Заявление на регистрацию и изготовление сертификата ключа подписи
(Приложение № 3 к Регламенту УЦ ООО «Кейсистемс»)

Ксерокопия паспорта лица, на которое выдаётся подпись.

Доверенность (Приложение №5 к Регламенту УЦ ООО «Кейсистемс»),
необходима только в случае, если подпись выдается не на «первое» лицо
организации.

Приложения к регламенту приведены ниже:

Приложение №3

к Регламенту Удостоверяющего центра ООО «Кейсистемс»
по созданию и управлению сертификатами ключей проверки электронной подписи,
используемыми для создания усиленной неквалифицированной электронной подписи
(Форма заявления на регистрацию и изготовление сертификата ключа)

Для юридических лиц

Заявление на регистрацию и изготовление сертификата ключа подписи Пользователя
в Удостоверяющем центре ООО «Кейсистемс»
(Распределенная схема обслуживания)

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____
просит зарегистрировать уполномоченного представителя в Реестре Удостоверяющего центра ООО «Кейсистемс»,
наделить полномочиями Пользователя Удостоверяющего центра ООО «Кейсистемс», установленными Регламентом
Удостоверяющего центра ООО «Кейсистемс» и сформировать ключи подписи и изготовить сертификат ЭП в
соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

| Общая информация | |
|-------------------------------------|------------------------------------|
| Полное наименование организации | |
| Краткое наименование организации | |
| ID запроса | |
| ИНН | |
| КПП | |
| ОГРН | |
| Город | |
| Область | |
| Адрес (улица, номер дома) | |
| e-mail | |
| | Информация о владельце сертификата |
| Ф.И.О (полностью) | |
| Должность | |
| Контактное лицо | |
| ФИО контактного лица | |
| Должность | |
| Телефон | |
| e-mail (для отправки сканов счетов) | |

Настоящим _____
(Фамилия, имя отчество владельца сертификата)

_____ (серия и номер паспорта, кем и когда выдан)
соглашается с обработкой своих персональных данных ООО «Кейсистемс» и признает, что персональные
данные, заносимые в сертификаты ключей проверки электронной подписи, относятся к общедоступным
персональным данным.

Подпись уполномоченного представителя (владельца сертификата) _____ / _____ /
подпись Ф.И.О.
« ____ » _____ 20__ г.

Наименование должности и Ф.И.О. руководителя организации:

_____ / _____ /
Должность подпись Ф.И.О.
« ____ » _____ 20__ г.
М.П.

Приложение №5

к Регламенту Удостоверяющего центра ООО «Кейсистемс»
по созданию и управлению сертификатами ключей проверки электронной подписи,
используемыми для создания усиленной неквалифицированной электронной подписи
(Форма доверенности Пользователя Удостоверяющего центра)

Для юридических лиц

Доверенность

г. _____ « ____ » _____ 20__ г.

_____ (полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____ (фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(фамилия, имя, отчество)

_____ (серия и номер паспорта, кем и когда выдан)

действовать от имени _____

_____ (полное наименование организации)

при использовании электронной подписи электронных документов, выступать в роли Пользователя Удостоверяющего центра ООО «Кейсистемс» и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «Кейсистемс» по созданию и управлению сертификатами ключей проверки электронной подписи, используемыми для создания усиленной неквалифицированной электронной подписи (Распределенная схема обслуживания), установленные для Пользователя Удостоверяющего центра ООО «Кейсистемс».

Настоящая доверенность действительна по* « ____ » _____ 20__ г.

Подпись уполномоченного представителя

(владельца сертификата)

_____ подтверждаю.

Ф.И.О.

подпись

Наименование должности и Ф.И.О. руководителя организации:

_____ Должность

_____ / _____ /
подпись Ф.И.О.

« ____ » _____ 20__ г.
М.П.

* Примечание: срок действия доверенности должен быть не менее срока действия ключа электронной подписи, соответствующего изготавливаемому сертификату.

Заполненные и подписанные документы отсканируйте и вышлите сканы на электронный адрес uc@keysystems.ru

Оригиналы вышлите по почтовому адресу: 428000, Чувашская республика, Чебоксары, главпочтамт, а/я172. ООО «Кейсистемс»

В ответ, по электронной почте, вы получите бланк акта выполненных работ.

Исполнитель:

ООО «Кейсистемс»
Юридический адрес: 428020, Чувашская Республика - Чувашия, г. Чебоксары, пр. И.Я.Яковлева, д. 3, нежилое помещение 22
Почтовый адрес: 428000, г. Чебоксары, Главпочтамт, а/я 172
ИНН 2128050753 / КПП 213001001
ОГРН 1032128012267
Р/с 40702810475020102693 в Отделении № 8613 Сбербанка России г. Чебоксары
К/с 30101810300000000609
БИК 049706609
Тел.: 8 (8352) 323-323, факс: 8 (8352) 571-033, e-mail: info@keysystems.ru

Заказчик:

ОБРАЗЕЦ

Акт № _____
по заявлению № б/н о присоединении к Регламенту Удостоверяющего центра ООО «Кейсистемс» от «___» _____ 20__ г.

г. Чебоксары

ДАТУ НЕ СТАВИТЬ

_____, именуемый
в дальнейшем «Заказчик», в лице _____,
действующего на основании _____, с одной стороны и ООО
«Кейсистемс», именуемое в дальнейшем «Исполнитель», в лице _____,

С регламентом Удостоверяющего центра ООО «Кейсистемс» можно ознакомиться по адресу:
<http://www.keysystems.ru/services/CertificationCentr/ReglamentRaspr.pdf>

Глава 3 Регистрация нового пользователя

Наберите в адресной строке <https://ra.keysystems.ru/ui/>.

Выберите «Начать регистрацию» Обратите внимание, что в ИНН юридического лица необходимо поставить в начале два ноля. Пример:0021212121. Заполните следующие поля:

Добро пожаловать на страницу самостоятельной регистрации!

Вам необходимо создать запрос на регистрацию в системе. Для этого заполните, пожалуйста, предлагаемую форму (обязательные поля помечены красным цветом).

| | |
|----------------------------|---------------------------------|
| Должность/звание: | Должность |
| Неструктурированное имя: | |
| Адрес: | Название Улицы и дом |
| Общее имя: | Фамилия Имя Отчество |
| Подразделение: | |
| Организация: | Название организации 64 символа |
| Город: | Населенный пункт |
| Область: | 00 Название области |
| Страна/регион: | RU |
| Электронная почта: | uc@keysystems.ru |
| ИНН: | 0021212121 |
| ОГРН: | 1234567891234 |
| СНИЛС: | 01234567890 |
| Ключевая фраза: | |
| Дополнительная информация: | |

Продолжить >>

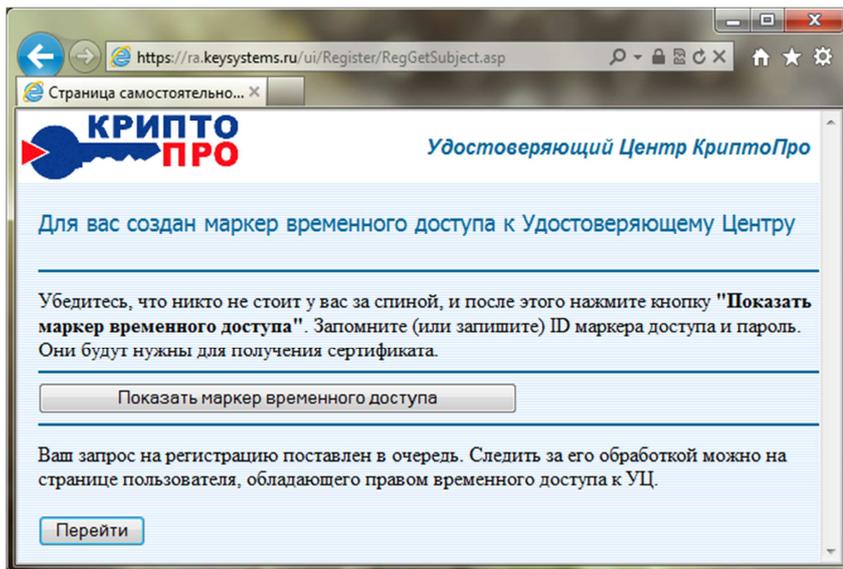
Поле «**Область**» заполняем **ПОЛНОСТЬЮ**. Например:

30 Астраханская область

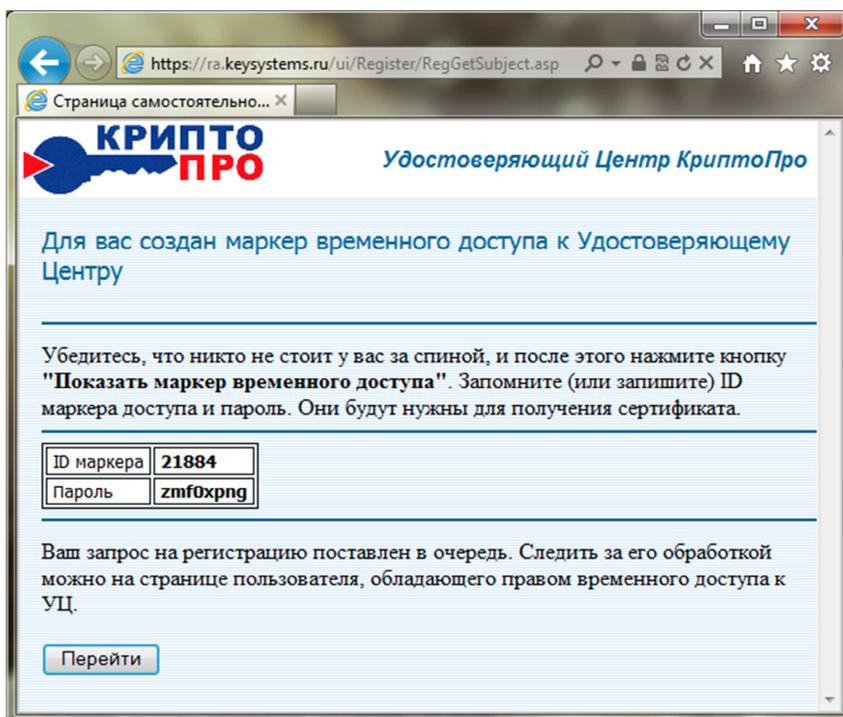
59 Пермский край

01 Республика Адыгея и т.д.

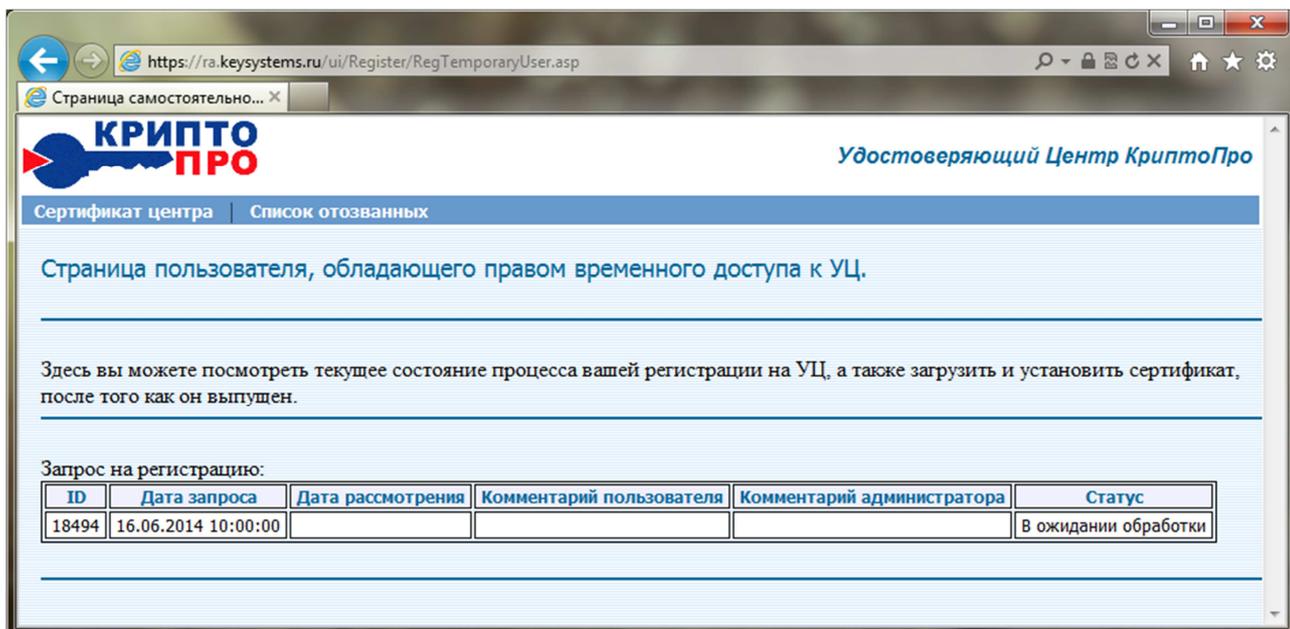
Нажмите «Продолжить»



Нажмите «Показать маркер временного доступа»



СКОПИРУЙТЕ и/или ЗАПИШИТЕ ID МАРКЕРА и ПАРОЛЬ
Нажмите «Перейти» и вы увидите статус вашего запроса на регистрацию



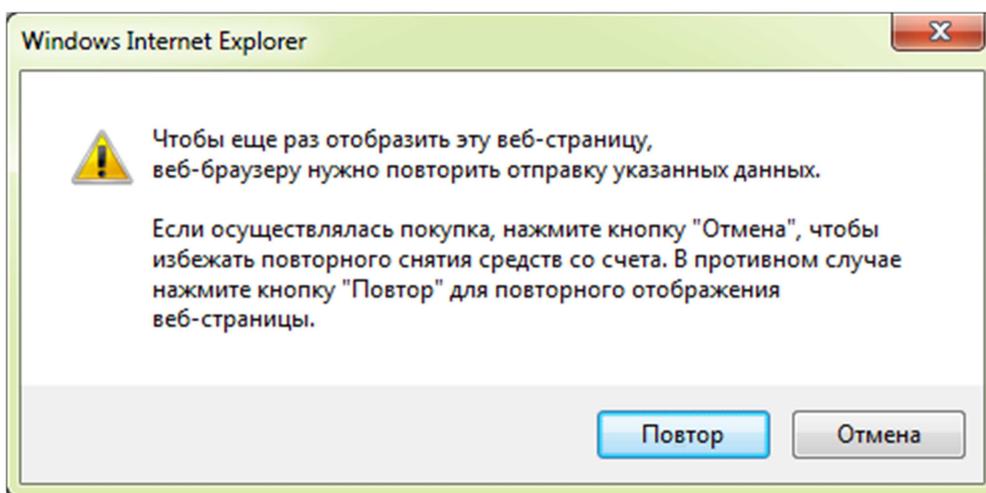
Ещё раз удостоверьтесь, направили ли вы на адрес uc@keysystems.ru заполненные и подписанные сканы документов.

Рекомендуемые параметры письма:

- расширение для направляемых файлов *.pdf, *.jpg, *.jpeg, *.bmp, *.png, *.gif;
- если файл архивируется, то в названии архива нужно указать ИНН организации;
- объем письма не более 10 Mb;
- **в теме письма - указание ИНН организации.**

Пожалуйста, отслеживайте сообщения в электронной почте, с которой были направлены документы. Возможно, Вам придёт сообщение от операторов Удостоверяющего Центра.

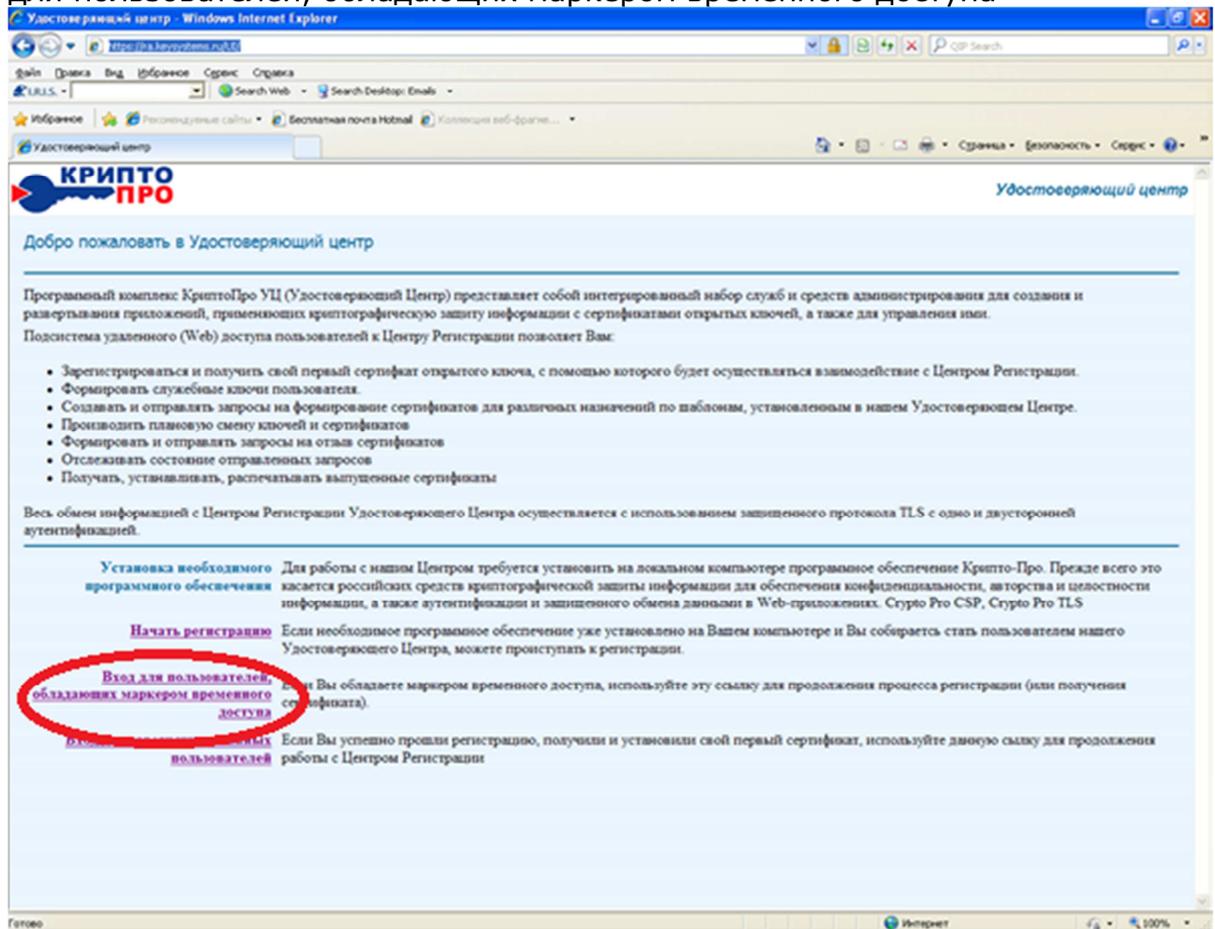
Периодически обновляйте страницу с состоянием запроса. Используйте кнопку F5 на клавиатуре. При обновлении страницы выходит сообщение.



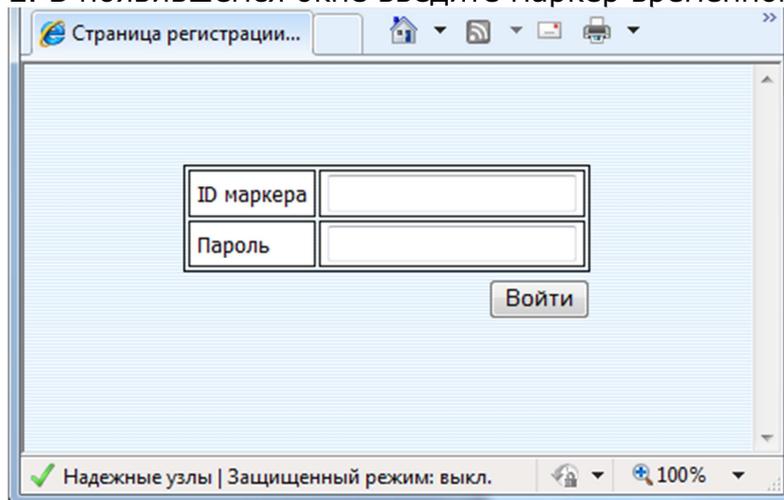
Нажмите «Повтор». Если Ваш запрос принят, то его статус изменится на «Завершен».

Глава 4 Формирование запроса на сертификат. Получение сертификата.

1. Зайдите на сайт <https://ra.keysystems.ru/ui/> и нажмите на ссылку «Вход для пользователей, обладающих маркером временного доступа»

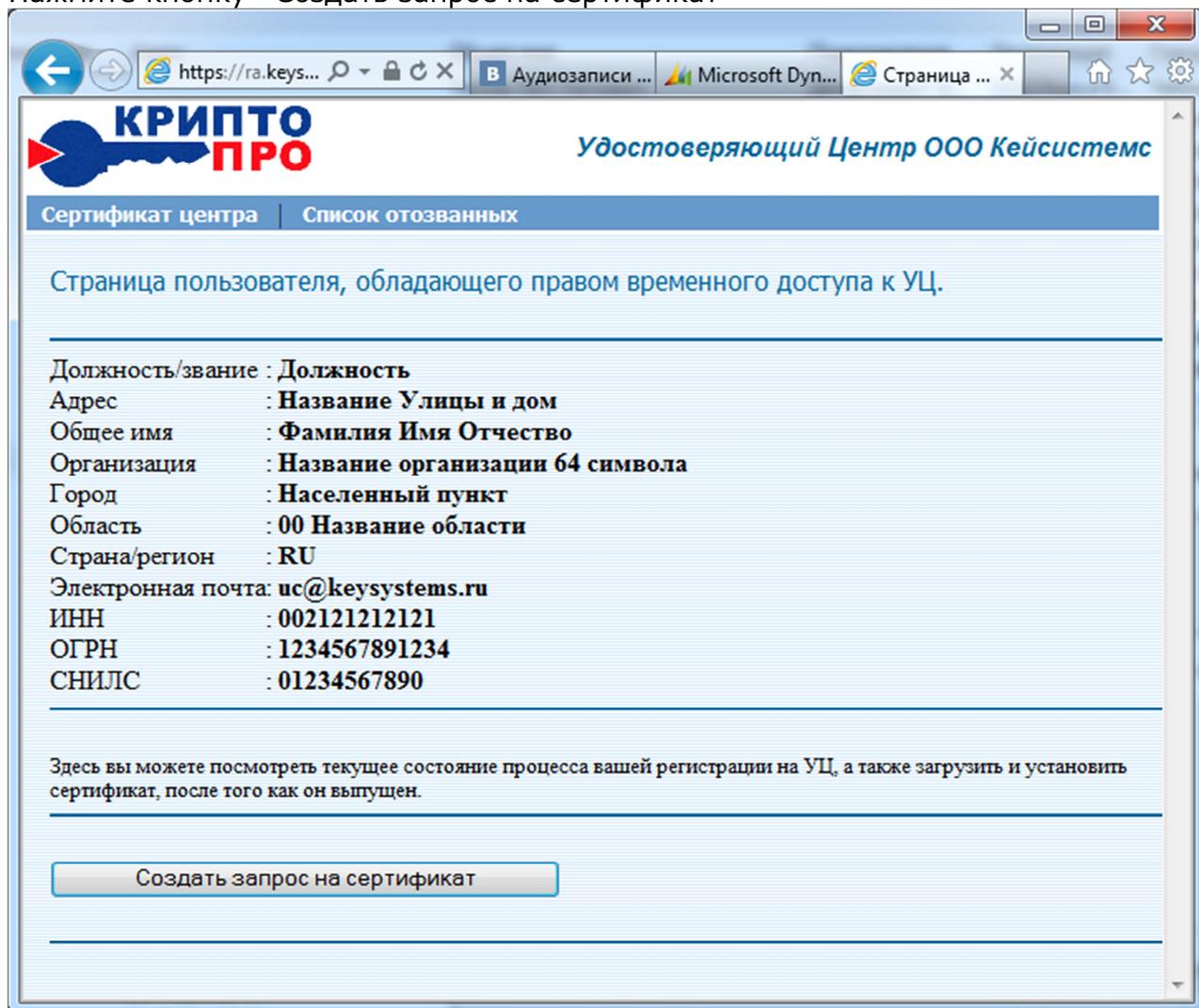


2. В появившемся окне введите маркер временного доступа и пароль.

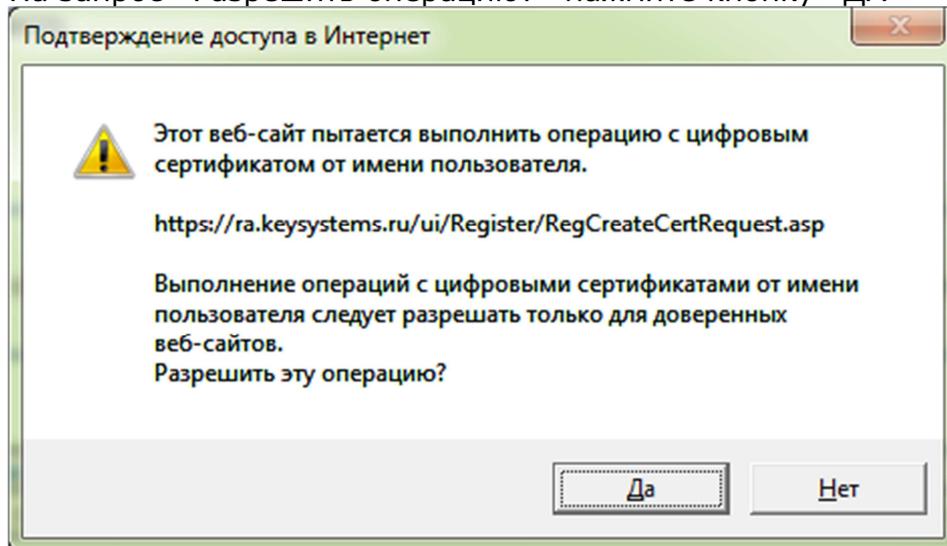


3. Вставьте РутOKEN  или E-token  в USB порт компьютера. **КРАЙНЕ НЕ РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ НЕСЕРТИФИЦИРОВАННЫЙ НОСИТЕЛЬ** (например, дискету или флешку). В ПРОТИВНОМ СЛУЧАЕ ВЫ РИСКУЕТЕ ЛИШИТЬСЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ.

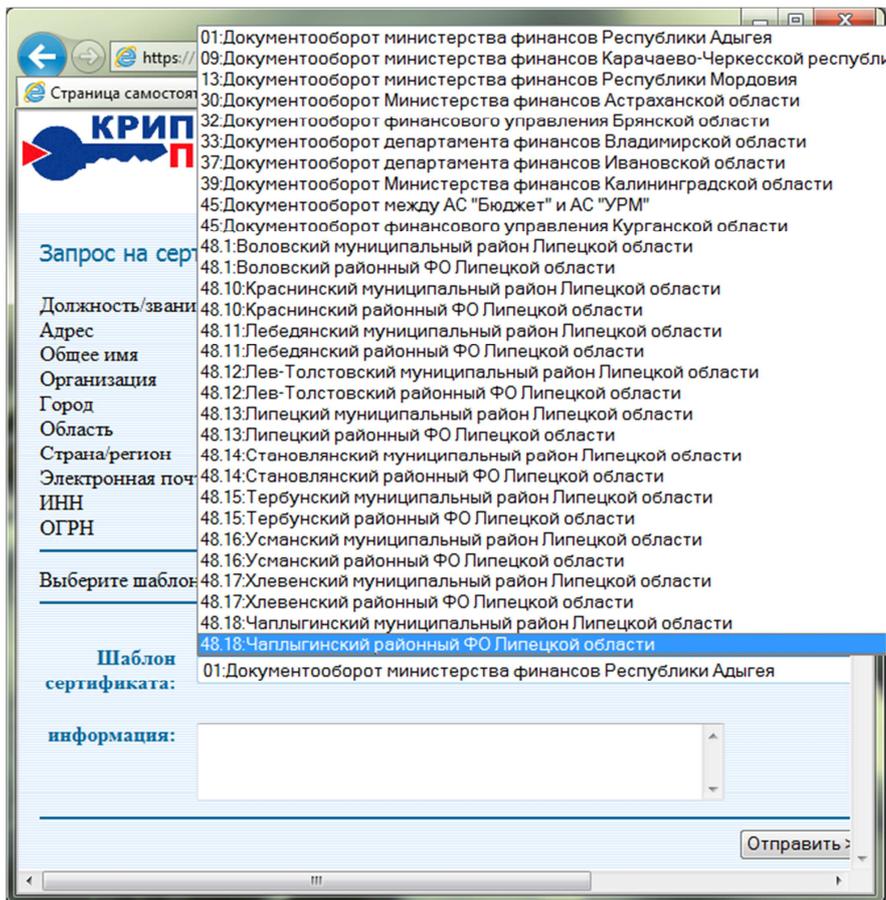
Нажмите кнопку «Создать запрос на сертификат»



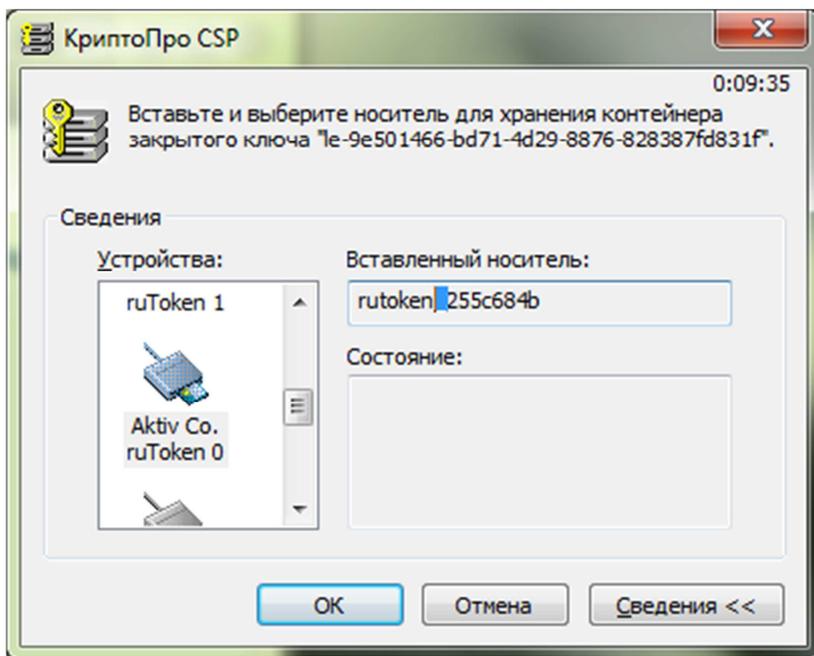
На запрос «Разрешить операцию?» нажмите кнопку «ДА»



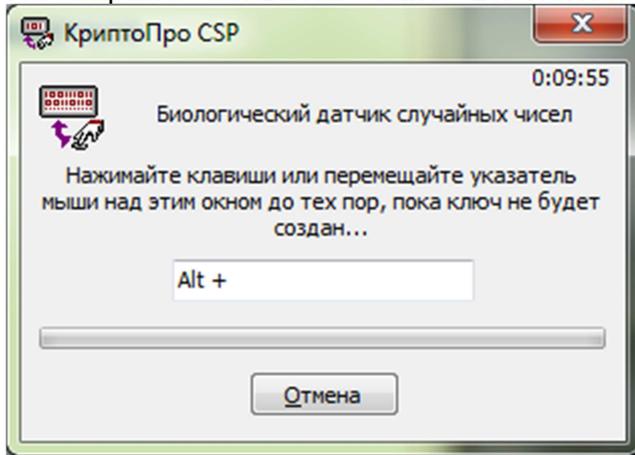
4. В появившемся окне в графе «Шаблон сертификата» выберете шаблон для своего региона и нажмите кнопку «Отправить»



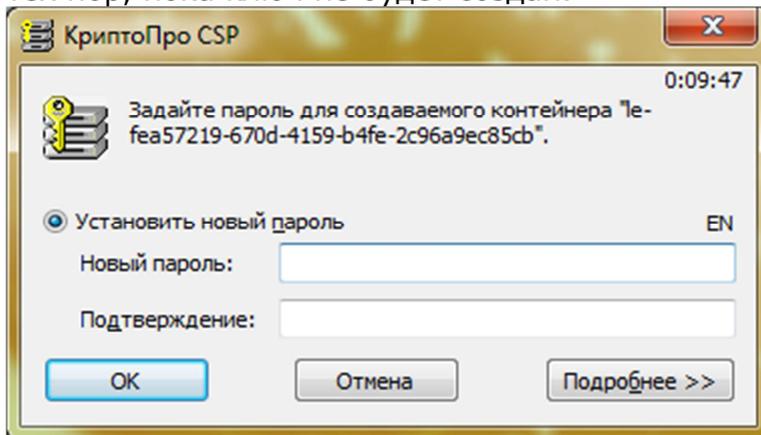
Выберите носитель для хранения ключа подписи и сертификата из предложенного списка в разделе «Устройства» (перемещайте ползунок, пока не найдете свой носитель).



На экране появится окно Биологического датчика случайных чисел.



Нажимайте клавиши или перемещайте указатель мыши над этим окном до тех пор, пока ключ не будет создан.

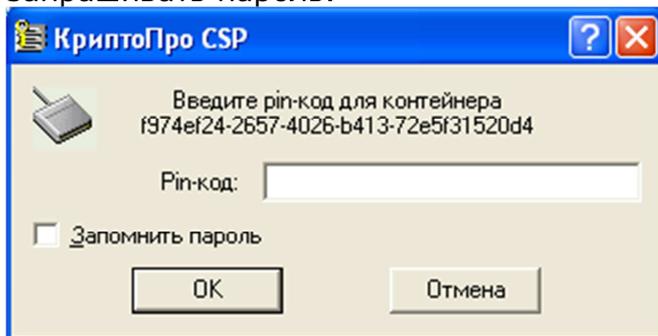


Вводите пароль на создаваемый контейнер и нажмите «ок».

Если подпись сделана на Рутокен  то заводской пароль на него 12345678

Если подпись сделана на E-token  то заводской пароль на него 1234567890

В дальнейшем, при использовании сертификата, система будет запрашивать пароль.



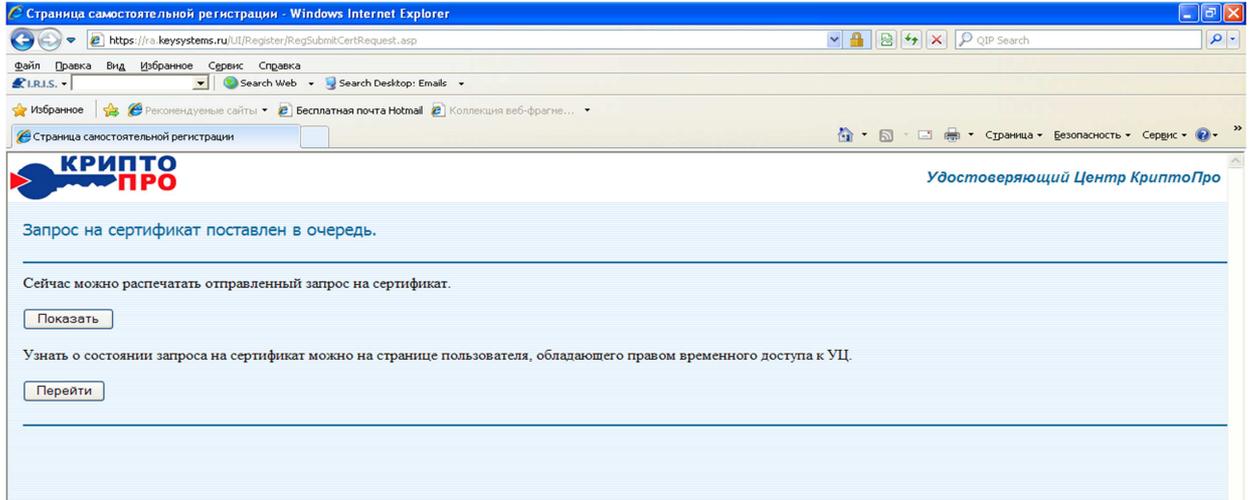
Для удобства использования можно поставить галочку в графе «Запомнить пароль».

НЕ ЗАБЫВАЙТЕ, ЧТО ПРИ НЕОДНОКРАТНОМ НЕПРАВИЛЬНО ВВЕДЕННОМ ПАРОЛЕ НОСИТЕЛЬ БЛОКИРУЕТСЯ. ПОСЛЕ БЛОКИРОВКИ ВОССТАНОВИТЬ СЕРТИФИКАТ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ БУДЕТ НЕВОЗМОЖНО.

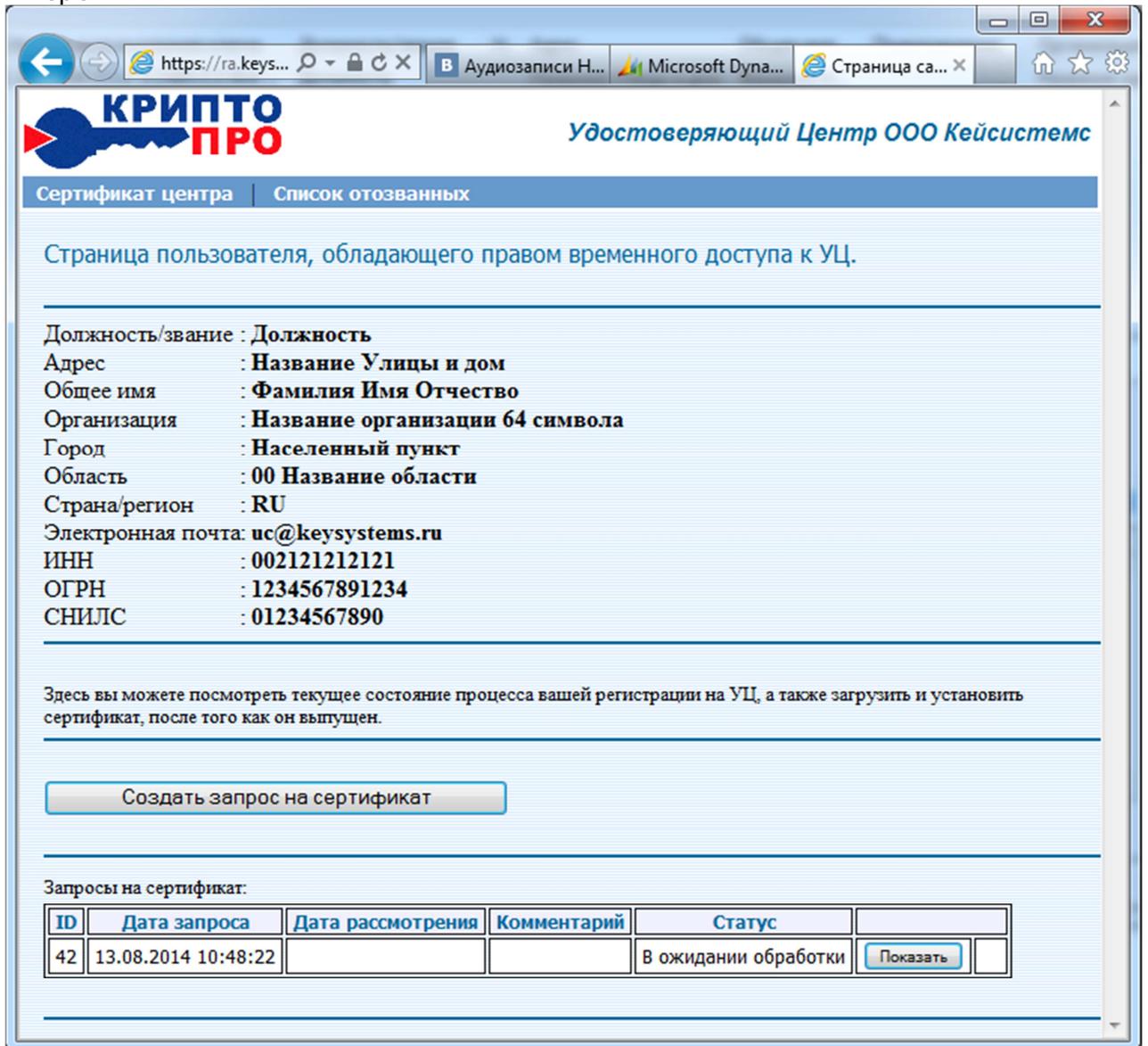
Количество попыток ввести пароль на Рутокен  -3

Количество попыток ввести пароль на E-token  -15

5. В появившемся окне нажмите «Показать»



6. Распечатайте появившийся бланк запроса, подпишите его и вместе с подписанным с вашей стороны актом выполненных работ отсканируйте и вышлите на uc@keysystems.ru. Закройте данное окно. Нажмите кнопку «Перейти».



Нажмите кнопку «Показать»

Запрос на сертификат X.509 - Windows Internet Explorer
https://ra.keysystems.ru/ui/Register/RegViewRequest.asp

Наименование организации-Удостоверяющего Центра
Запрос на сертификат ключа проверки электронной подписи

Сведения о запросе на сертификат:
Кем выпущен:
Фамилия Имя Отчество

Версия: 1 (0x0)

Субъект запроса на сертификат: T = Должность, STREET = Название Улицы и дом, CN = Фамилия Имя Отчество, O = Название организации 64 символа, L = Населенный пункт, S = 00 Название области, C = RU, E = uc@keysystems.ru, ИНН = 0021212121, ОГРН = 1234567891234, СНИЛС = 01234567890

Ключ проверки электронной подписи:
Алгоритм ключа проверки электронной подписи:
Название: ГОСТ Р 34.10-2001
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 4D55 820D 3661 C6AD 7BFF 88B9 C380 5A65 9BFE 487C 7F55 A3D5 FAB7 EB31 6EE8 3C71 5456 8CEF 31C9 4E94 68AA D46D 371A 4CA0 034F 72B6 6B36 1289 0803 5683 96D0 4FEF

Атрибуты запроса на сертификат X.509

- Атрибут 1.3.6.1.4.1.311.13.2.3
Название: Версия ОС
Значение: 6.1.7601.2
- Атрибут 1.3.6.1.4.1.311.21.20
Название: Сведения о клиенте
Значение: 30 44 02 01 05 0c 17 6b 73 2d 33 36 34 2e 6b 65 79 73 79 73 74 65 6d 73 2e 6c 6f 63 61 6c 0c 12 4b 45 59 53 59 53 54 45 4d 53 5c 62 65 6c 6f 76 61 6e 0c 12 43 65 72 74 45 6e 72 6f 6c 6c 43 74 72 6c 2e 65 78 65
- Атрибут 1.2.840.113549.1.9.14
Название: Расширения сертификатов
Расширения сертификата X.509
 - Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
 - Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Класс средства ЭП КС1 (1.2.643.100.113.1) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Электронный документооборот Министерства финансов Астраханской области (1.2.643.3.93.5) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
 - Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: 92 d5 03 e7 e9 84 69 de c8 c0 83 d5 f9 d7 f7 b4 d2 e2 f0 c8
- Атрибут 1.3.6.1.4.1.311.13.2.2
Название: CSP подачи заявок
Сведения о провайдере
Назначение ключа : ОБМЕН
Название провайдера : Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Подпись провайдера :

Подпись запроса:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Значение: 3F69 2788 06D8 D2A4 381D 01CA 8483 94AA 938F 1335 6044 BE3B 2864 CBE4 1186 55FB 5F96 1804 13CA 12CC 174A 533B 2782 B187 C51B AB3D AF6B 12AB 2D7A 374F 0DB9 464F

Подпись владельца запроса на сертификат: _____ / _____
" ____ " _____ 20__ г.

Проверьте данные в запросе. Распечатайте его, подпишите и поставьте печать организации.

Проверьте полученный по электронной почте от операторов Удостоверяющего Центра Акт, распечатайте его, подпишите, поставьте печать организации.

ВНИМАНИЕ: НЕ СТАВЬТЕ ДАТУ АКТА.

Акт № ____
по заявлению № б/н о присоединении к Регламенту Удостоверяющего центра ООО
«Кейсистемс» от «__» _____ 20__ г.

г. Чебоксары

ДАТУ НЕ СТАВИТЬ

_____, именуемый
в дальнейшем «Заказчик», в лице _____,
действующего на основании _____, с одной стороны и ООО
«Кейсистемс», именуемое в дальнейшем «Исполнитель», в лице
_____,
действующего на основании _____, с другой
стороны, именуемые также «Стороны», действующие на основании заявления № б/н о
присоединении к Регламенту Удостоверяющего центра ООО «Кейсистемс» от «__»
_____ 20__ г. (Регистрационный № _____ от «__» _____ 20__ г. в реестре
Удостоверяющего центра) составили настоящий акт о нижеследующем:

1. В соответствии с заявлением Удостоверяющий центр изготовил Уполномоченному
представителю сертификат ключа подписи (клиентский сертификат ключа подписи) в
количестве 1 шт.

2. Стоимость услуг составляет _____ (_____) рублей 00
копеек, в том числе НДС 18% _____ (_____) рублей ____ копеек.

3. Следует к перечислению на расчетный счет Исполнителя сумма в размере _____
(_____) рублей 00 копеек, в том числе НДС 18% _____ (_____) рублей ____ копеек.

4. Настоящий Акт составлен в 2 (Двух) экземплярах, имеющих одинаковую юридическую
силу, по одному для каждой из сторон.

От Исполнителя

М. П.

От Заказчика

М. П.



Оба документа вышлите по электронной почте uc@keysystems.ru.

7. Дождитесь, когда в разделе «Запросы на сертификат» «Статус» изменится на «Завершен» и появится кнопка «Получить сертификат».

КРИПТО ПРО Удостоверяющий Центр ООО Кейсистемс

Сертификат центра | Список отозванных

Страница пользователя, обладающего правом временного доступа к УЦ.

Должность/звание : Должность
 Адрес : Название Улицы и дом
 Общее имя : Фамилия Имя Отчество
 Организация : Название организации 64 символа
 Город : Населенный пункт
 Область : 00 Название области
 Страна/регион : RU
 Электронная почта: uc@keysystems.ru
 ИНН : 0021212121
 ОГРН : 1234567891234
 СНИЛС : 01234567890

Здесь вы можете посмотреть текущее состояние процесса вашей регистрации на УЦ, а также загрузить и установить сертификат, после того как он выпущен.

Создать запрос на сертификат

Запросы на сертификат:

| ID | Дата запроса | Дата рассмотрения | Комментарий | Статус | |
|----|---------------------|---------------------|-------------|----------|--------------------------------|
| 42 | 13.08.2014 10:48:22 | 13.08.2014 10:50:23 | | Завершен | Показать Получить сертификат |

Подтверждение доступа в Интернет

 Этот веб-сайт пытается выполнить операцию с цифровым сертификатом от имени пользователя.

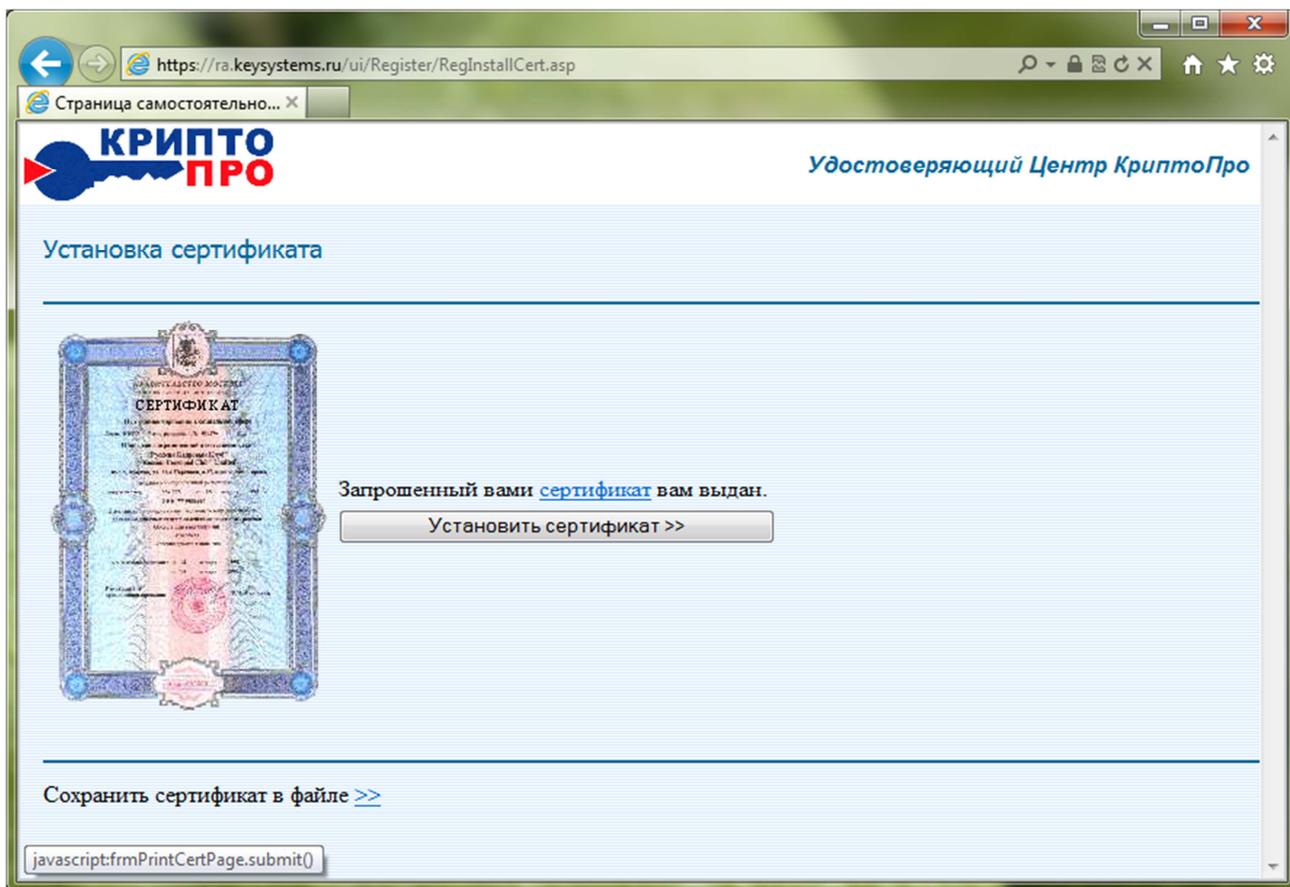
<https://ra.keysystems.ru/ui/Register/RegInstallCert.asp>

Выполнение операций с цифровыми сертификатами от имени пользователя следует разрешать только для доверенных веб-сайтов.

Разрешить эту операцию?

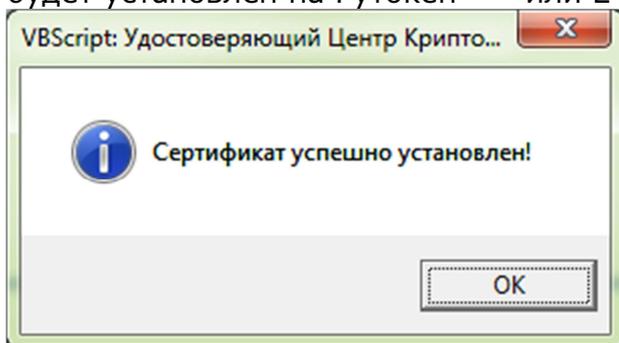
Да Нет

На запрос «Разрешить операцию?» нажмите кнопку «Да».



Нажмите ссылку «Сертификат», распечатайте бланк сертификата в двух экземплярах (один экземпляр отправьте по почте с полным комплектом документов).

Нажмите кнопку «Установить сертификат», и выданный Вам сертификат будет установлен на Рутокен  или E-token .



С ЭТОГО МОМЕНТА ВАША ПОДПИСЬ ДЕЙСТВУЕТ.