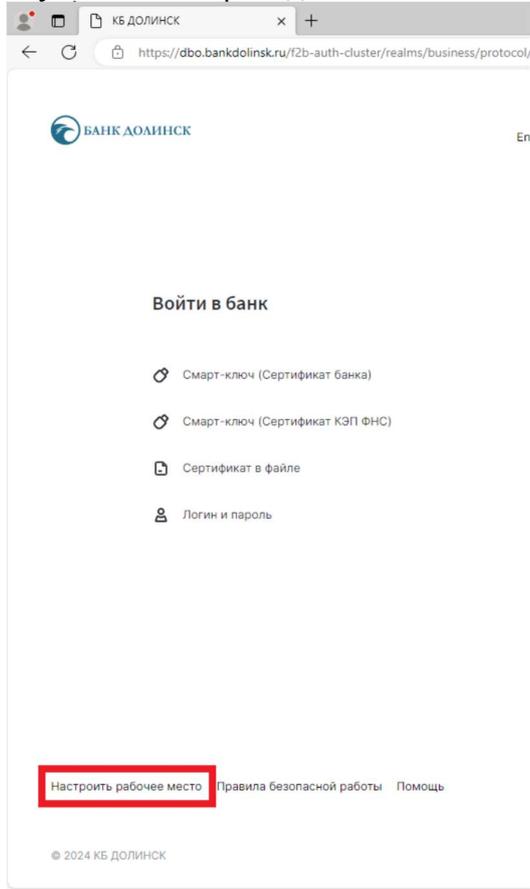
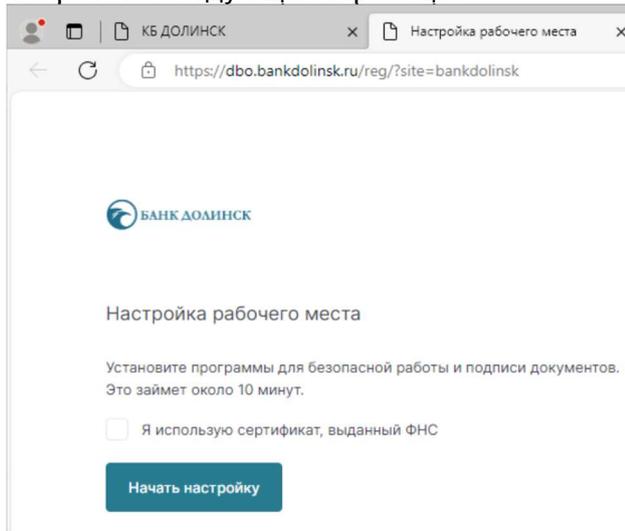


Для начала работы в ДБО Faktura посредством авторизации через «Сертификат» необходимо скачать и установить пакет ПО, содержащий в своём составе драйвера для СКЗИ типа Рутокен, консоли управления и необходимые плагины к браузерам.

Необходимо перейти на сайт <https://dbo.bankdolinsk.ru/> и в нижней его части осуществить переход по ссылке «Настроить рабочее место»:

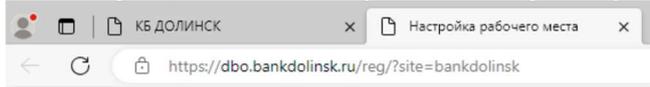


Откроется следующая страница:



Необходимо нажать кнопку «Начать настройку». **Отмечаем**, что корректная работа в ДБО возможно только в интернет браузерах Chrome, Microsoft Edge или Яндекс-Браузер!

На следующем этапе настройки Вам будет предложено установить расширение для браузера:



Настройка рабочего места

2 / 3 Установка расширения

Расширение «Интернет-банк Faktura.ru» нужно для корректной работы электронной подписи

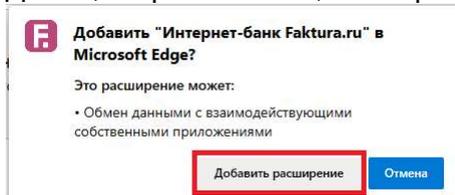
[Установить расширение](#)

После нажатия кнопки «Установить Расширение» откроется новая страница/вкладка браузера со следующим содержанием:

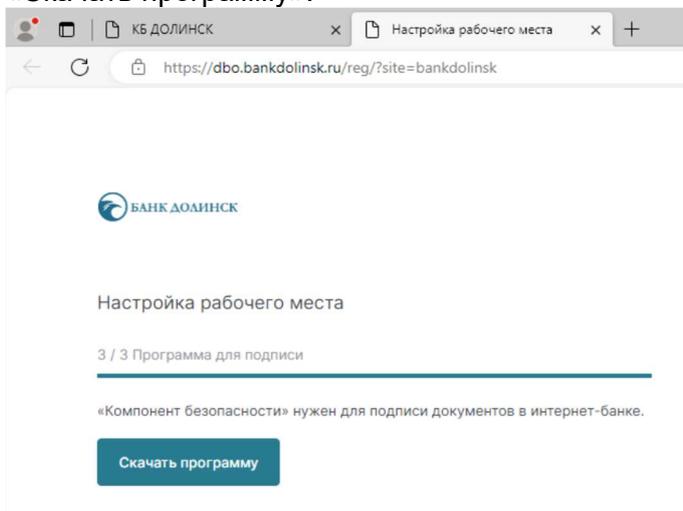


Необходимо нажать «Получить»:

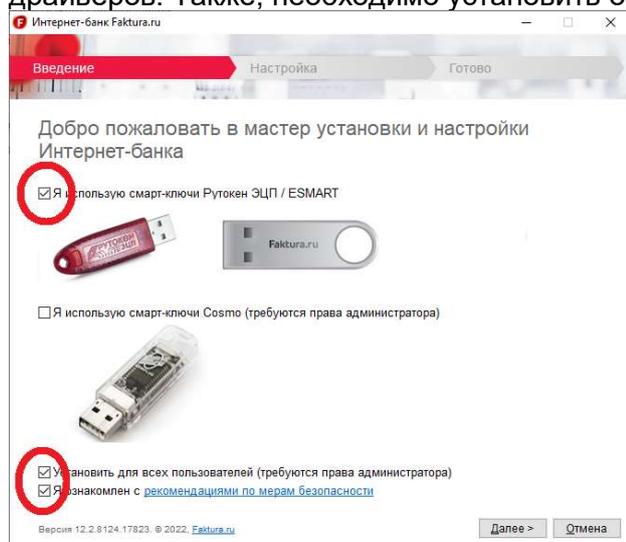
Далее, откроется окно, в котором нужно выбрать пункт «Добавить расширение»:



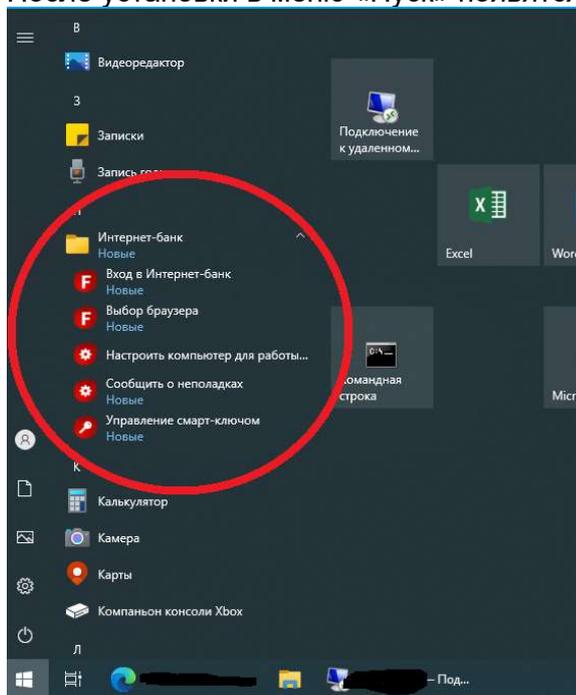
После успешной установки, необходимо вернуться к странице/вкладке браузера с выполняемой настройкой рабочего места. На следующем шаге, Вам будет предложено «Скачать программу»:



После загрузки объемного дистрибутива (около 86 Мб.), необходимо запустить установщик. Целесообразно запускать его с правами администратора, т.к. происходит установка драйверов. Также, необходимо установить отмеченные галочки:



После установки в меню «Пуск» появятся следующие ярлыки:



Также, на рабочем столе будет создан ярлык «Вход в Интернет-банк». Желательно перезагрузить ПК после выполнения установки ПО. На этом подготовительный этап заканчивается.

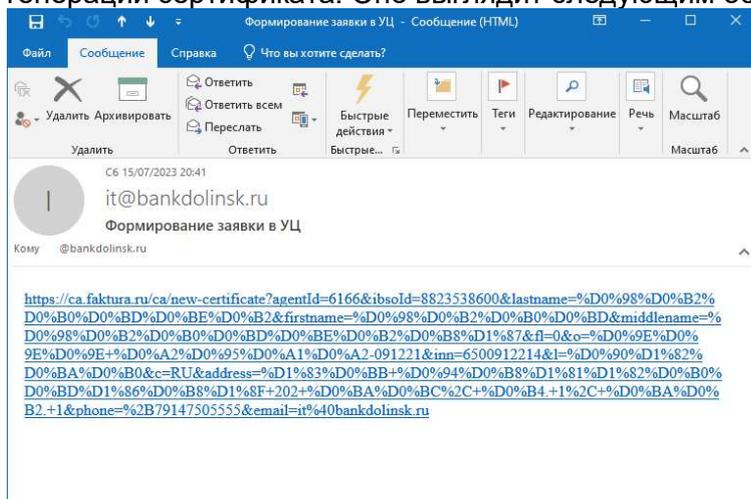
Далее необходимо осуществить выпуск сертификата электронной подписи. Процесс выполняется в два этапа.

На первом этапе осуществляется его генерация. После успешного выполнения этапа в банк отправляется уведомление/запрос на выпуск сертификата электронной подписи.

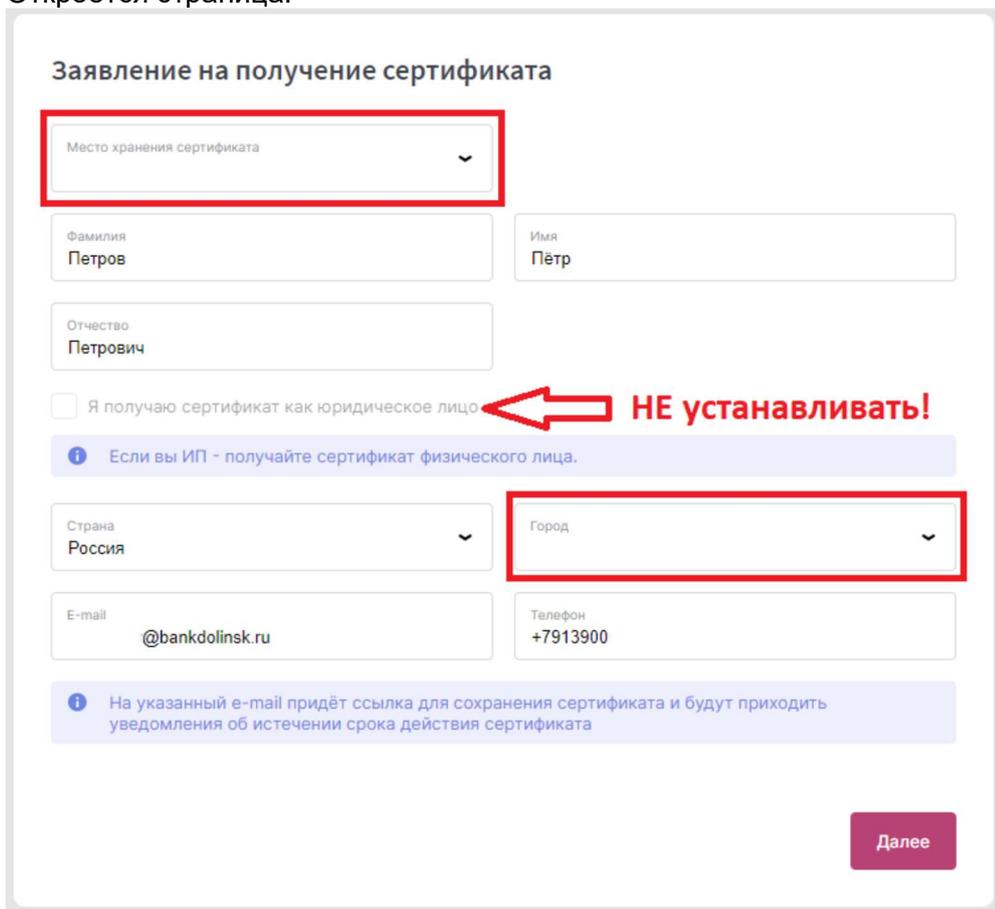
На втором этапе, в удостоверяющем центре банка выполняется подтверждение Вашего сертификата. В результате чего, Вам направляется сообщение на электронную почту о его готовности и необходимости загрузки.

Первый этап.

Вам поступит электронное сообщение в почту, содержащее ссылку, необходимую для генерации сертификата. Оно выглядит следующим образом:



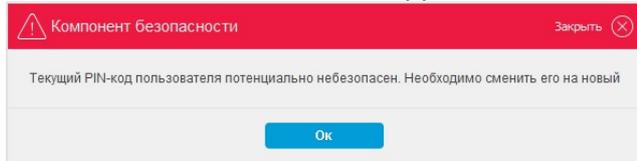
Необходимо подключить выданный в банке USB токен и перейти по ссылке. Откроется страница:



The screenshot shows a web form titled "Заявление на получение сертификата". The form includes several input fields: "Место хранения сертификата" (highlighted with a red box), "Фамилия" (Петров), "Имя" (Пётр), "Отчество" (Петрович), "Страна" (Россия), "Город" (highlighted with a red box), "E-mail" (@bankdolinsk.ru), and "Телефон" (+7913900). A checkbox labeled "Я получаю сертификат как юридическое лицо" is present, with a red arrow pointing to it and the text "НЕ устанавливать!". A blue information box below the checkbox states: "Если вы ИП - получайте сертификат физического лица." At the bottom right, there is a "Далее" button.

Большинство полей уже будут заполнены! Необходимо выбрать из выпадающего списка «Место хранения сертификата» - смарт ключ. **Внимание! Устанавливать галочку в поле «Я получаю сертификат как юридическое лицо» - недопустимо!** Также, необходимо убедиться в правильности указанных данных и дополнительно проверить поле E-mail, т.к. именно на него будут приходить все уведомления и статусы по сертификатам ЭЦП.

После, необходимо нажать «Далее». Появится окно:

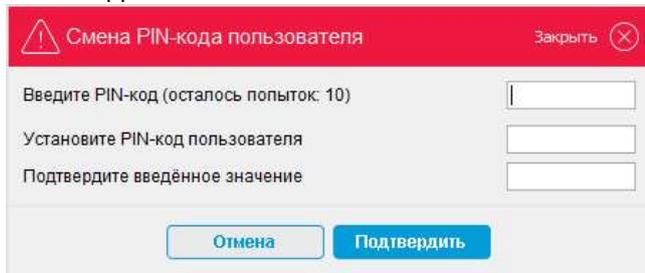


Компонент безопасности Закреть ✕

Текущий PIN-код пользователя потенциально небезопасен. Необходимо сменить его на новый

Ок

Необходимо нажать «ОК».



! Смена PIN-кода пользователя Закреть ✕

Введите PIN-код (осталось попыток: 10)

Установите PIN-код пользователя

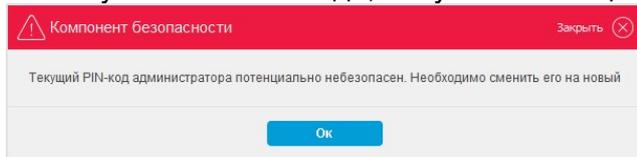
Подтвердите введенное значение

Отмена Подтвердить

PIN-код **ПОЛЬЗОВАТЕЛЯ** по умолчанию – **12345678**

Далее устанавливаем новый PIN-код (не менее восьми символов), который необходимо придумать. **Внимание**, если Вы его забудете, Вам будет необходимо выполнить генерацию сертификата снова, т.к. банк не контролирует этот PIN-код и не сможет его Вам подсказать/сменить/сбросить!

После установки PIN-кода, получаем сообщение:

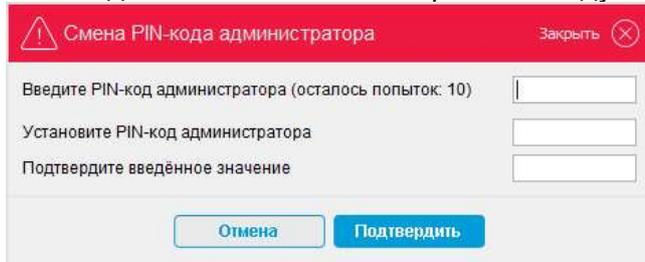


Компонент безопасности Закреть ✕

Текущий PIN-код администратора потенциально небезопасен. Необходимо сменить его на новый

Ок

Необходимо нажать «ОК». Откроется следующее окно:



! Смена PIN-кода администратора Закреть ✕

Введите PIN-код администратора (осталось попыток: 10)

Установите PIN-код администратора

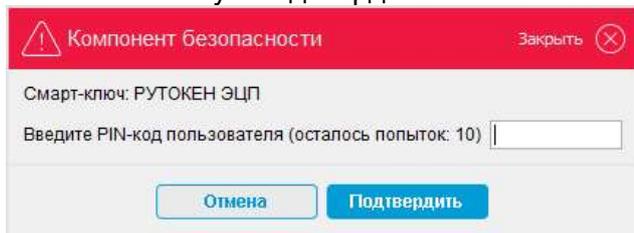
Подтвердите введенное значение

Отмена Подтвердить

PIN-код **АДМИНИСТРАТОРА** по умолчанию – **87654321**

Вводим придуманный новый PIN-код **АДМИНИСТРАТОРА** (не менее восьми символов). **Внимание**, если Вы его забудете, Вам будет необходимо выполнить генерацию сертификата сначала, т.к. банк не контролирует этот PIN-код и не сможет его Вам подсказать/сменить/сбросить!

Нажмите кнопку «Подтвердить». Появится сообщение:



! Компонент безопасности Закреть ✕

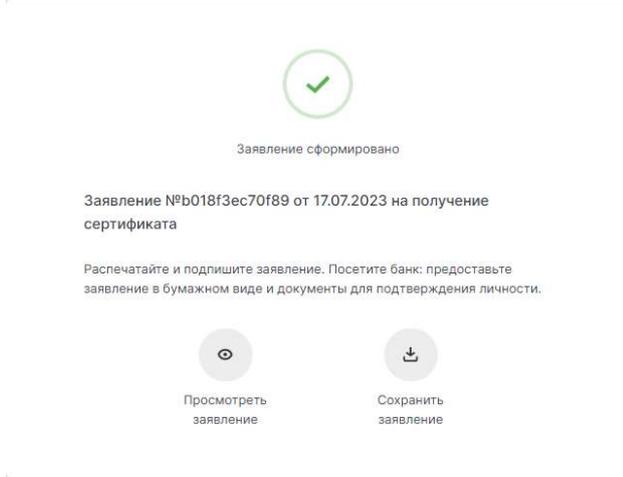
Смарт-ключ: РУТОКЕН ЭЦП

Введите PIN-код пользователя (осталось попыток: 10)

Отмена Подтвердить

ВНИМАНИЕ, на этом этапе необходимо ввести **ТОЛЬКО ЧТО УСТАНОВЛЕННЫЙ** PIN-код **ПОЛЬЗОВАТЕЛЯ!**

После ввода Вашего PIN-кода пользователя, откроется окно браузера с уведомлением:



Необходимо распечатать заявление в двух экземплярах (через кнопку просмотреть заявление)!

Агенту Удостоверяющего центра «AUTHORITY»
«Наименование Агента»
/ в Удостоверяющий центр «AUTHORITY»

Заявление на выдачу Сертификата ключа проверки электронной подписи

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать мне Сертификат ключа проверки электронной подписи (Класс Сертификата) для физического лица с параметром Идентификатора владельца сертификата: (ФИО / псевдоним Клиента). Уникальный номер запроса: _____.

С Правилами Электронного документооборота корпоративной информационной Системы «BeSafe» (далее – «Система «BeSafe»), которые размещены в сети Интернет на сайте www.besafe.ru ознакомлен(-а), согласен(-на) и обязуюсь соблюдать и выполнять.

Принимаю, что получение документа, подписанного Электронной подписью Участника Системы «BeSafe» (далее – «Участник») юридически эквивалентно получению документа на бумажном носителе, подписанного собственноручными подписями уполномоченных лиц Участника и заверенного печатью Участника, если документ на бумажном носителе должен быть заверен печатью. Обязательства, установленные настоящим пунктом, действительны при условии, что Ключ электронной подписи, Электронная подпись и Сертификат ключа проверки электронной подписи Участника созданы и используются в соответствии с Правилами работы Удостоверяющего центра «AUTHORITY».

Реквизиты Клиента:

ФИО	
Контактный номер телефона	
E-mail	

Настоящим соглашаюсь с обработкой своих персональных данных, в том числе с использованием технических средств. Закрытым акционерным обществом «Центр Цифровых сертификатов», а также Агентом (Доверенным лицом) Удостоверяющего центра «AUTHORITY».

Принимаю, что мои персональные данные, включенные в Сертификат, будут внесены Удостоверяющим центром в реестр Сертификатов. Реестр Сертификатов доступен в сети Интернет на сайте www.authority.ru.

Понимаю, что Удостоверяющий центр обрабатывает мои персональные данные, включенные в Сертификат и размещенные в реестре Сертификатов, для выполнения обязанностей по ведению реестра Сертификатов, включенно содержащихся в Сертификатах персональных данных в реестр Сертификатов и обеспечению доступа лиц к информации, содержащейся в реестре Сертификатов с использованием сети Интернет, которые возложены на Удостоверяющий центр частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Понимаю, что в соответствии с пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» выполнение Удостоверяющим центром обязанностей, возложенных на него частью 2 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», является правовым основанием обработки моих персональных данных, включенных в Сертификат.

_____ (подпись Клиента) / _____ (Ф.И.О. Клиента)

принято Агентом Удостоверяющего центра / Удостоверяющим центром:

_____ (полное наименование)

_____ (дата)

_____ (подпись уполномоченного лица)

_____ (ФИО уполномоченного лица, реквизиты доверенности)

М.П.

Также, отмечаем, что при нажатии кнопки «Сохранить заявление», происходит загрузка бланка заявления на компьютер (что полезно, если есть необходимость распечатки документа где-то на другом рабочем месте).

Оригиналы заявлений доставляются в банк для проверки и подписания.

На этом первый этап выпуска сертификата электронной подписи завершен. Окна браузера необходимо закрыть, USB носитель извлечь из компьютера и убрать на хранение. После отправки заявлений и выполнения всех необходимых процедур на стороне банка, на указанный клиентом e-mail адрес поступит сообщение, в котором будут указаны дальнейшие шаги.

Второй этап.

Вам поступит электронное сообщение на почту следующего вида:

Вам выдан сертификат в КБ "Долинск" (АО) для работы в Интернет-Банке.
Загрузить и сохранить его можно [здесь](#).

Необходимо, вставить USB носитель и перейти по ссылке (щелкнуть по гиперссылке «здесь»).
Откроется страница браузера:

Удостоверяющий центр "AUTHORITY" (ЗАО "ЦЦС")

Сохранение сертификата

Сохраните сертификат и предоставьте в банк акт приема-передачи:

1. Проверьте данные сертификата и введите пароль.
2. Сохраните сертификат.
3. Распечатайте и подпишите акт приема-передачи сертификата.
4. Отправьте подписанный акт приема-передачи в банк

Сохранить сертификат

Далее, нажмите на кнопку «Сохранить сертификат». Откроется страница:

Данные сертификата

Место хранения сертификата
Смарт-ключ (ГОСТ)

Убедитесь что смарт-ключ подключен!

Владелец
CN=Ivanov

Удостоверяющий центр
CN=Class 2 CA, O=Center of Financial Technologies, C=RU

Серийный номер
8c550

Уникальный номер запроса
b018f

Сохранить сертификат

Необходимо ещё раз нажать «Сохранить сертификат».
Будет продемонстрировано сообщение:

Компонент безопасности Закреть

Смарт-ключ: РУТОКЕН ЭЦП

Введите PIN-код пользователя (осталось попыток: 10)

Отмена Подтвердить

Вам необходимо ввести PIN-код **ПОЛЬЗОВАТЕЛЯ**. После чего будет показано сообщение:

