Установка торгового терминала Quik и формирование ключей шифрования

Содержание

1 Общая информация

1.1 Назначение документа

Документ описывает порядок формирования ключей шифрования и электронной подписи.

1.2 Поддержка

Оперативное решение проблем при работе с Системой QUIK осуществляется с 9:30 до 18:30 по московскому времени. В остальное время осуществляется регистрация обращений, которые будут незамедлительно решены с утра следующего рабочего дня.

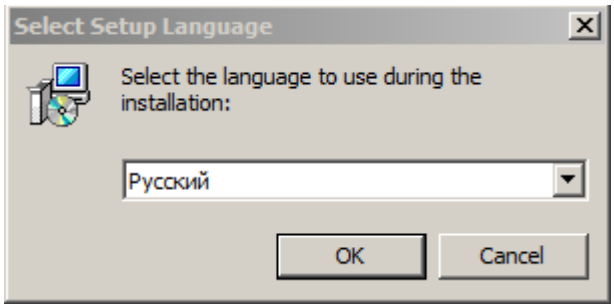
Телефон: +7 (495) 775-77-17

E-mail: **quik@raiffeisen.ru**

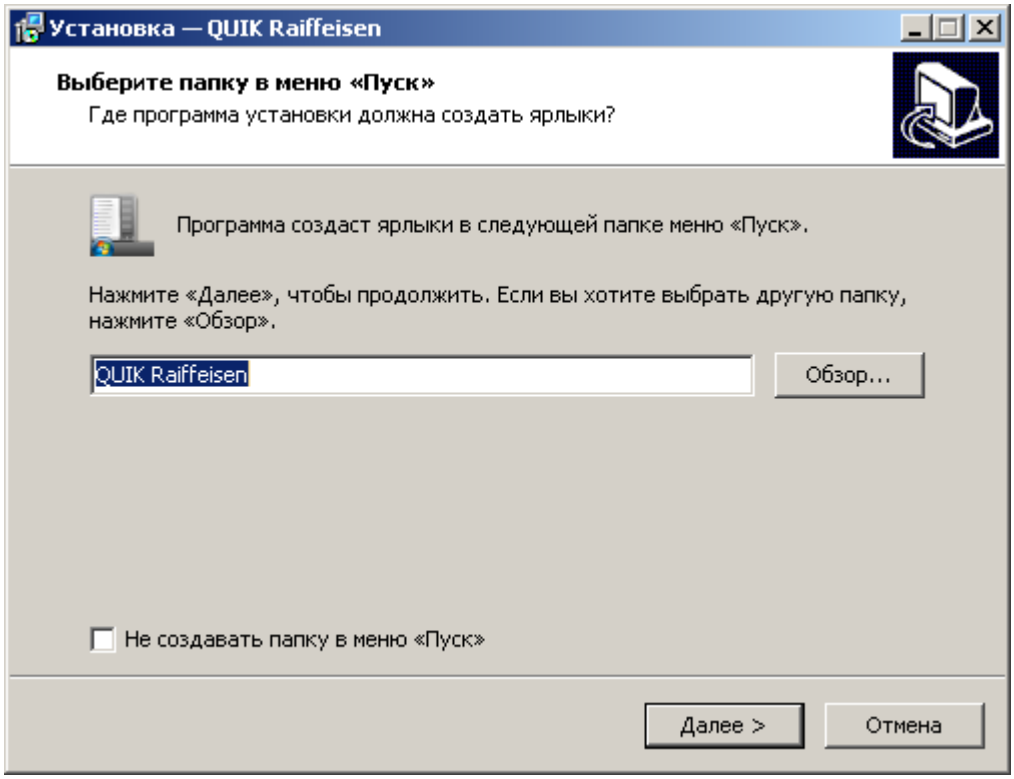
2 Установка приложения.

Загрузите дистрибутив программы QUIK по ссылке: http://www.raiffeisen.ru/common/img/uploaded/files/QUIK_setup.exe и запустите файл установщик QUIK_setup.exe.

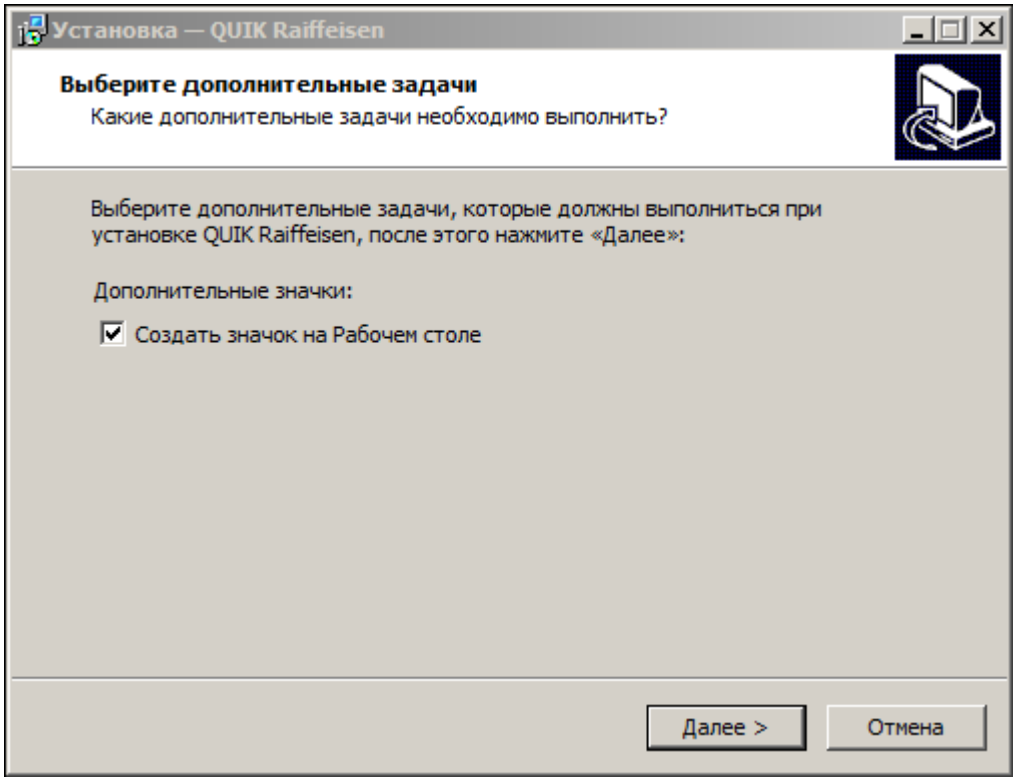
В появившемся окне необходимо выбрать язык для установки приложения и нажать кнопку «OK»:



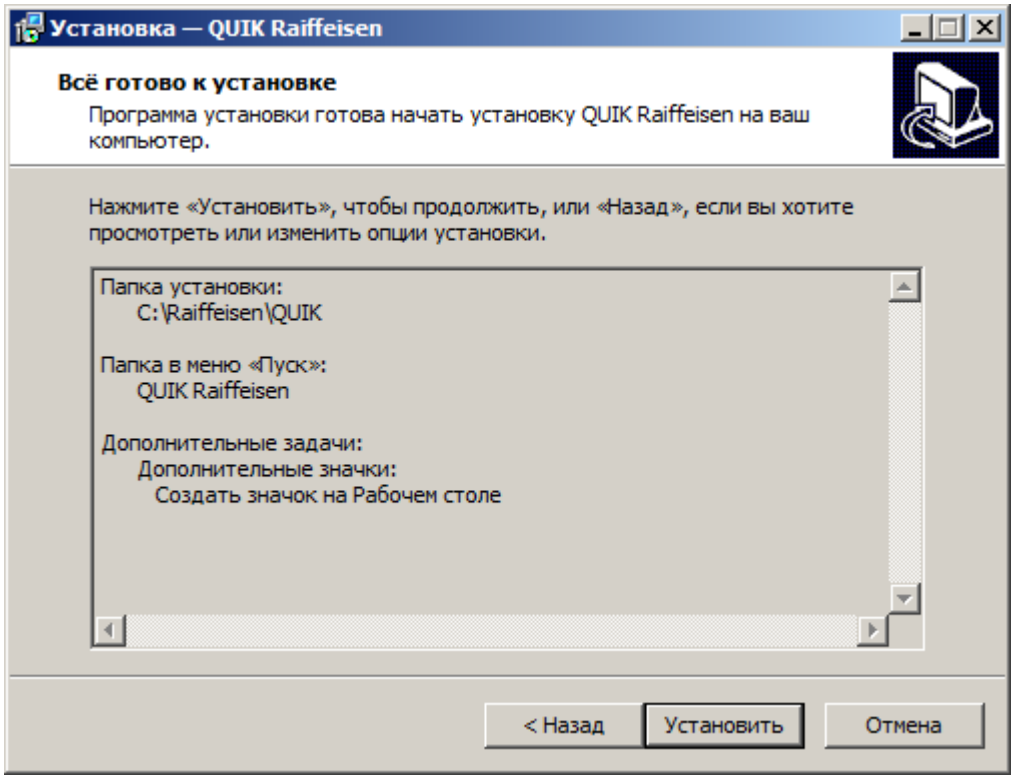
Для продолжения установки нажмите кнопку **«Далее»**



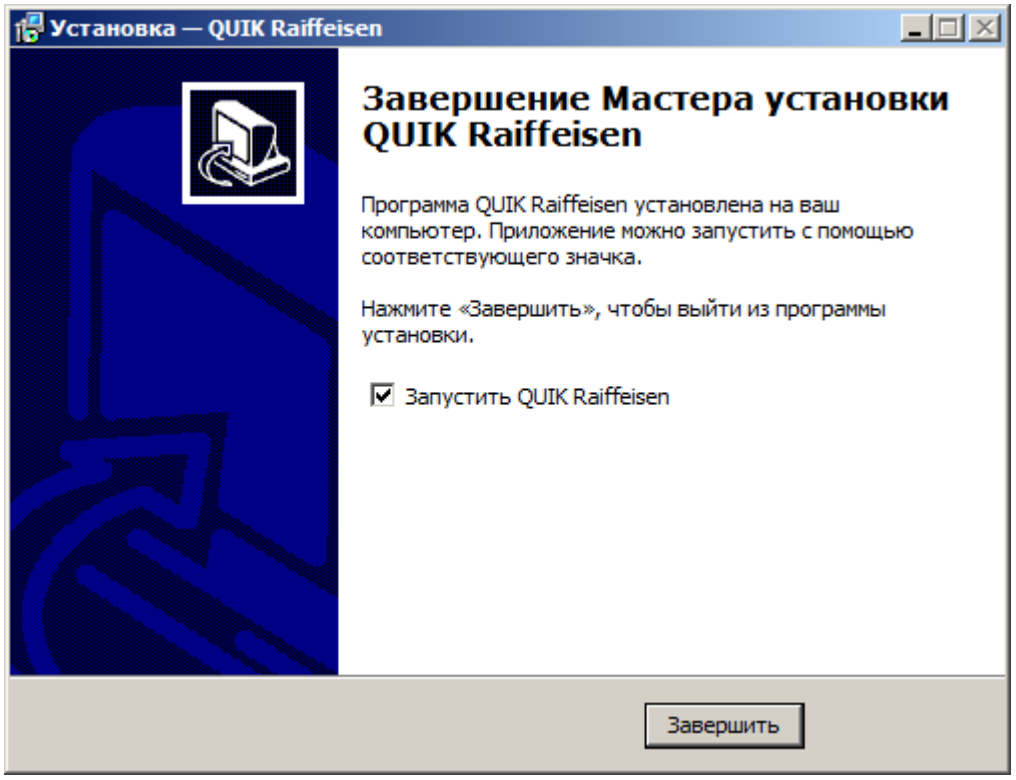
В появившемся окне необходимо установить опцию **«Создать значок на Рабочем столе»** и нажать кнопку **«Далее»**



Нажмите кнопку **«Установить»**



Результатом успешной установки будет окно **«Завершение Мастера установки QUIK Raiffeisen»**, в данном окне нажмите **«Завершить»**

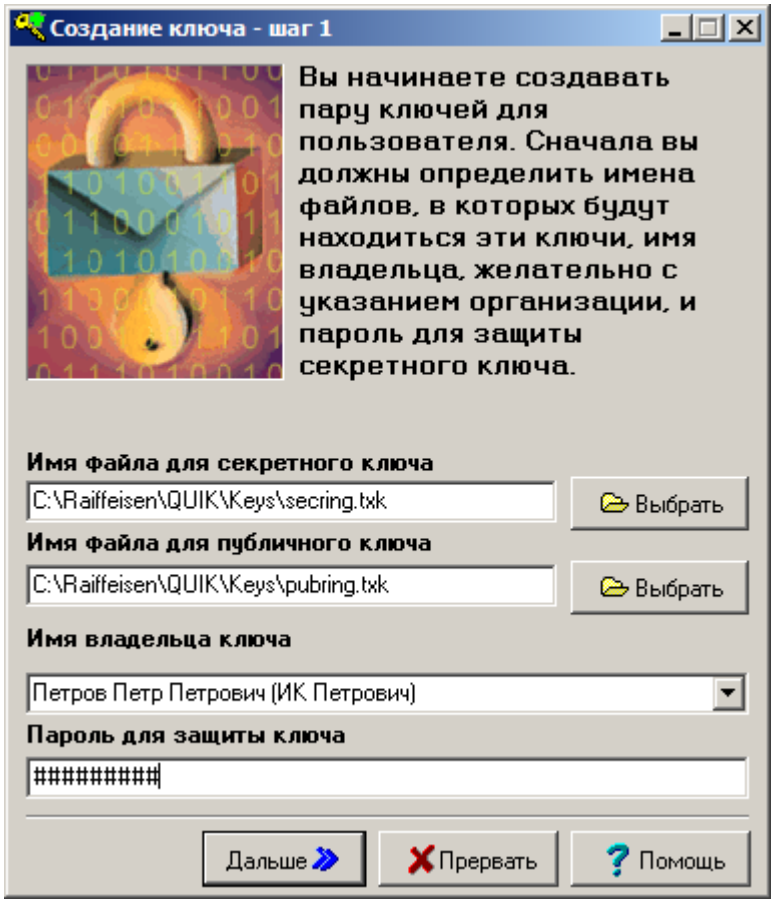


3 Формирование ключей шифрования

Для начала формирования ключа шифрования Вам необходимо запустить приложение KeyGen из меню «Пуск» (по умолчанию Пуск/Все программы/QUIK Raiffeisen/KeyGen)

3.1 Формирование имени и пароля.

На первом шаге создания ключа выбираются имена файлов для открытой (pubring.txk) и секретной (secring.txk) части создаваемого ключа, имя его владельца и пароль для защиты секретной части ключа. Имя владельца ключа используется для регистрации пользователя на сервере и авторизации пользователя при подключении (Логин в систему QUIK). Пароль защищает секретную часть ключа пользователя от несанкционированного использования (секретная часть ключа хранится в файле secring.txk в зашифрованном виде, и при вводе логина и пароля пользователь запускает процедуру её расшифровки).



В поле **«Имя файла для секретного ключа»** пропишите директорию, где будет храниться закрытая часть ключа шифрования.

В поле **«Имя файла для публичного ключа»** пропишите директорию, где будет храниться открытая часть ключа шифрования.

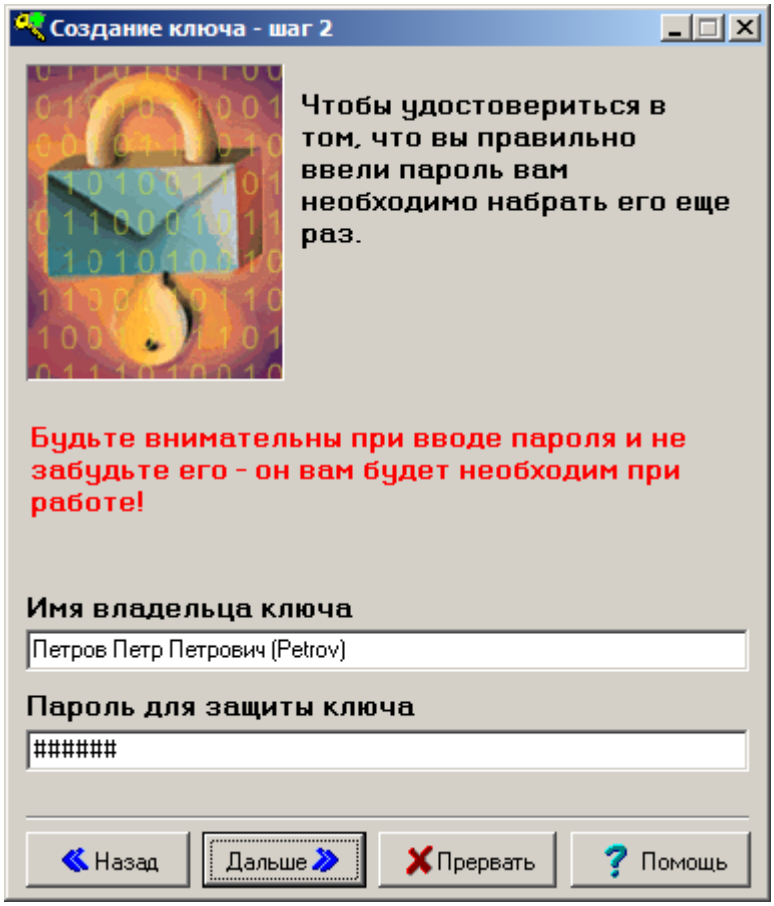
В поле **«Имя владельца ключа»** пропишите ФИО пользователя системы. В скобках необходимо указать фамилию пользователя латиницей, данное значение будет использоваться в качестве логина в систему.

В поле **«Пароль для защиты ключа»** укажите пароль, данный пароль будет использоваться для входа в систему.

После заполнения всех полей нажмите кнопку **«Дальше»**

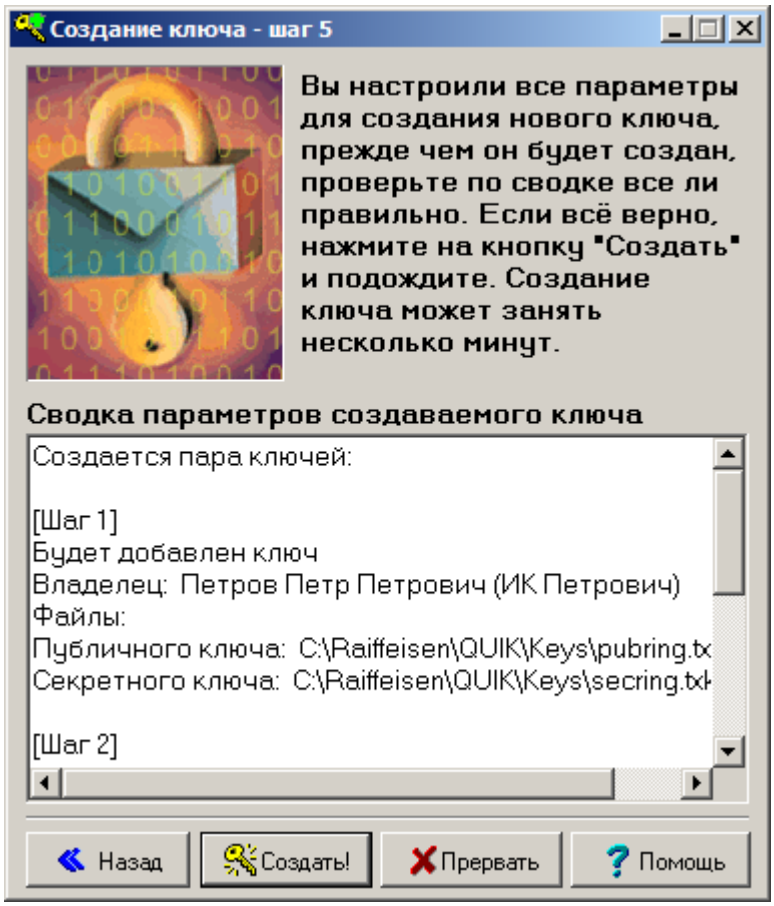
3.2 Подтверждение пароля

В появившемся окне необходимо подтвердить ранее введённый пароль. После подтверждения пароля нажмите кнопку **«Дальше»**



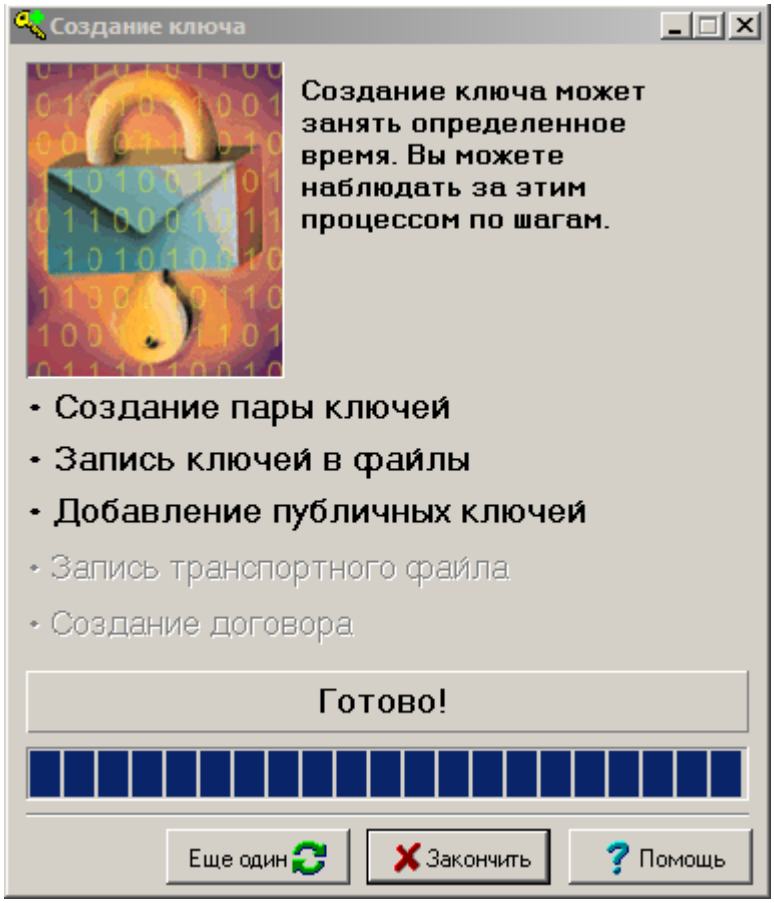
3.3 Подтверждение параметров ключа

В появившемся окне необходимо проверить корректность введённых для создания ключа данных и нажать кнопку **«Создать!»** для завершения формирования ключа.



3.4 Завершение

Результатом успешного создания ключа будет появившееся окно:



После успешного создания ключа нажмите кнопку **«Закончить»**.

4 Передача открытого ключа шифрования.

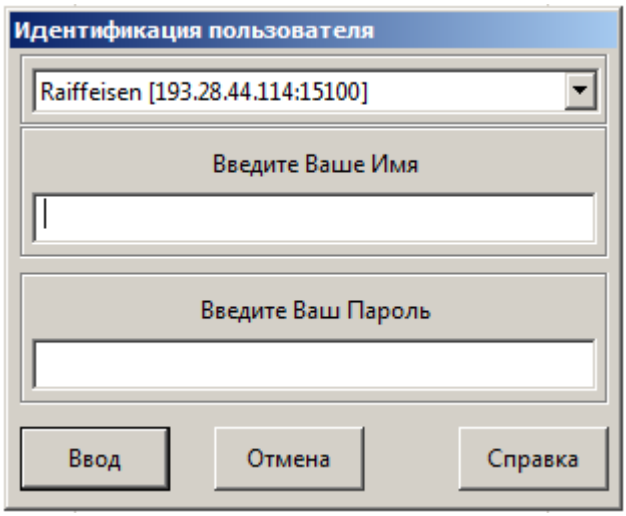
После успешного создания ключей шифрования, направьте письмо с темой: **«Keys: ИКИ»** на адрес электронной почты **quik@raiffeisen.ru**. **ИКИ – это** Идентификационный код Инвестора (номер Соглашения), указанного в Уведомлении об открытии счетов.

Письмо должно содержать файл открытой части ключа шифрования, путь по умолчанию: **C:\Raiffeisen\QUIK\Keys\pubring.txk**

ОБРАТИТЕ ВНИМАНИЕ, что для регистрации пользователя в системе закрытая часть ключа (secring.txk) не нужна. Вся процедура генерации закрытой и открытой частей ключа рассчитана на то, что закрытая часть не должна передаваться третьим лицам. В случае компрометации ключей шифрования процедуру генерации придётся повторить. Понятие «Компрометация» представлено в договоре на использование системы QUIK.

5 Запуск приложения.

После запуска приложения в окне **«Идентификация пользователя»** введите имя пользователя и пароль, которые были сформированы в п. 3.1 настоящей инструкции, и нажмите кнопку **«Ввод»**



В появившемся окне **«Двухфакторная аутентификация»** введите пароль доступа (PIN), полученный через SMS сообщение и нажмите кнопку **«Ввод»**