Подготовка компьютера к работе в системе интернет-банк «Faktura»

ВНИМАНИЕ!!! Для работы в системе интернет-банк «Faktura» необходимо использовать браузер (интернет-обозревателя) Internet Explorer 11 или Google Chrome

1. Откройте браузер и перейдите по ссылке: **https://business.faktura.ru/f2b/faq?article=2-1**

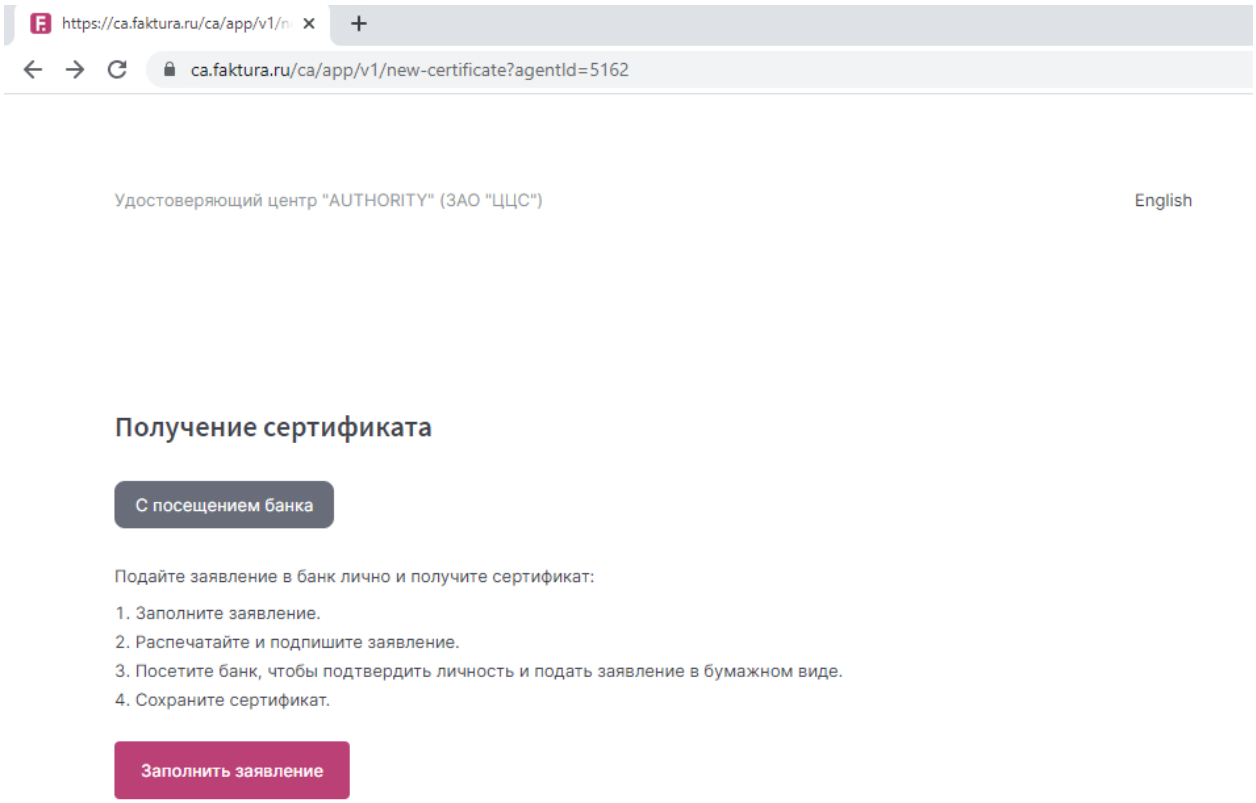
2. Скачайте программное обеспечение для Windows 7, 8, 10.
3. Запустите файл мастера настройки **≪InternetBankSetup.exe≫.**
4. Следуйте дальнейшим указаниям в окне установки.
5. Нажмите ≪Завершить≫ по завершении установки.
6. Если для работы используется браузер Google Chrome – дополнительно установите расширение.

Получение личного сертификата безопасности для работы в системе интернет-банк «Faktura»

ВНИМАНИЕ!!! Все нижеописанные действия необходимо выполнять с использованием браузера (интернет-обозревателя) Internet Explorer 11 или Google Chrome

Шаг 1. Установить считыватель со смарт-картой в USB-порт рабочей станции (компьютера).
Шаг 2. Начать процедуру создания личного сертификата, ввести (скопировать) ссылку в адресную строку браузера:

https://ca.faktura.ru/ca/new-certificate?agentId=5162



После нажатия кнопки «Заполнить заявление» появится регистрационная форма (рисунок 1).

Шаг 3. Заполнить регистрационную форму (рисунок 1): указать устройство хранения сертификата - **Смарт-ключ (ГОСТ)**, нажать кнопку «Подтвердить». Система предложит ввести секретный PIN-код (рисунок 2).

ВНИМАНИЕ!!! PIN-код пользователь придумывает и вводит самостоятельно, его необходимо запомнить и не сообщать сторонним лицам.

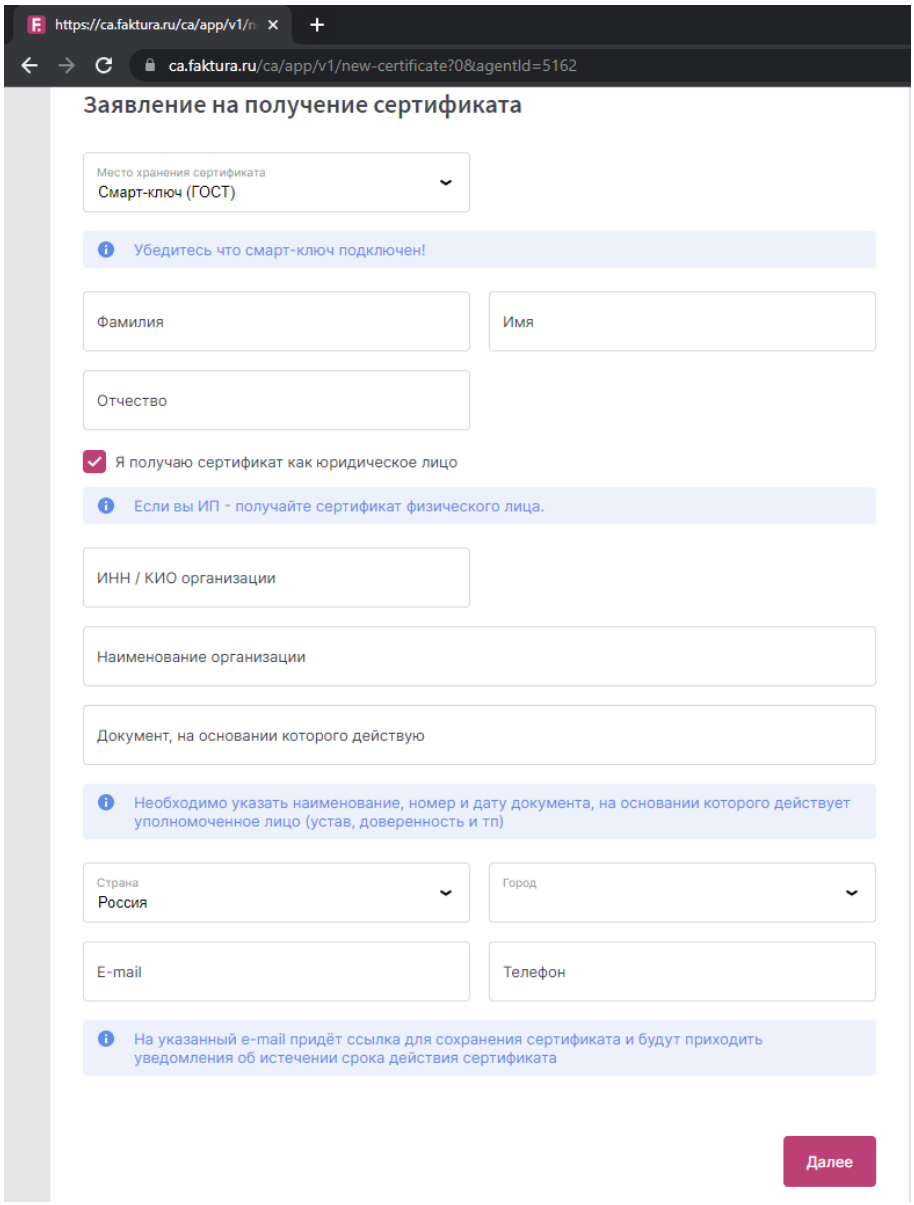


Рисунок 1

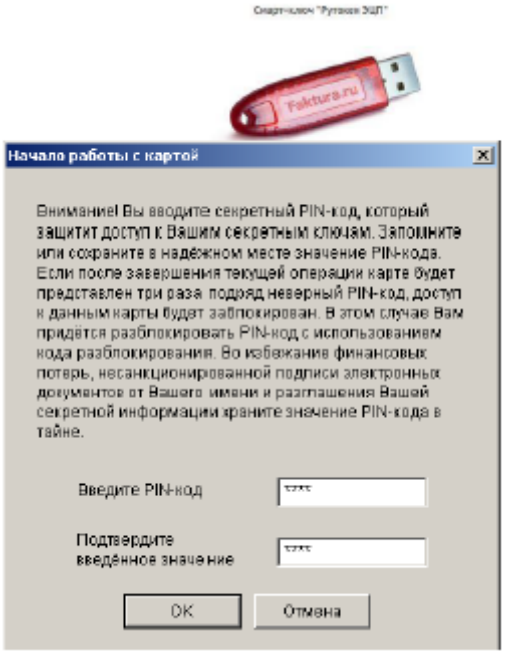


Рисунок 2

ВНИМАНИЕ!!! В случае использования смарт-ключа Рутокен-ЭЦП (красный ключ с надписью Faktura.ru) по умолчанию установлен пароль пользователя –«12345678», пароль администратора – «87654321»

Шаг 4. Далее необходимо задать код разблокирования (нужен в случае троекратного ошибочного ввода PIN-кода) (рисунок 3).

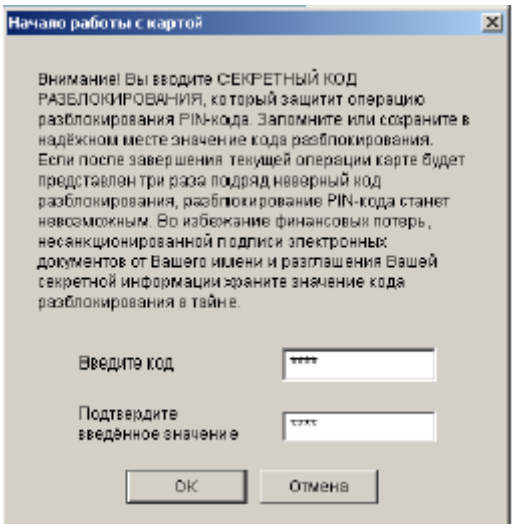


Рисунок 3

ВНИМАНИЕ!!! В случае троекратного неверного ввода секретного кода (PIN-кода) смарт- карта блокируется. Разблокировка производится с помощью кода разблокирования. В случае троекратного неверного ввода кода разблокирования смарт-карта более не может быть использована в дальнейшем.

Шаг 5. После создания PIN-кода и кода разблокирования система повторно запросит PIN-код (Рисунок 4)

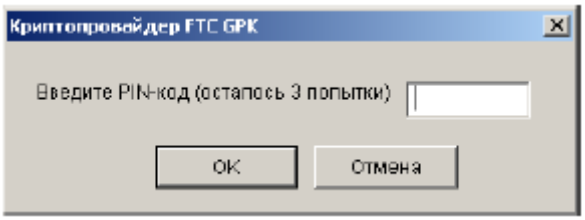


Рисунок 4

Шаг 5.1 При первом обращении к Рутокену система предложит вам сменить **PIN-код пользователя** нажимайте **ОК**

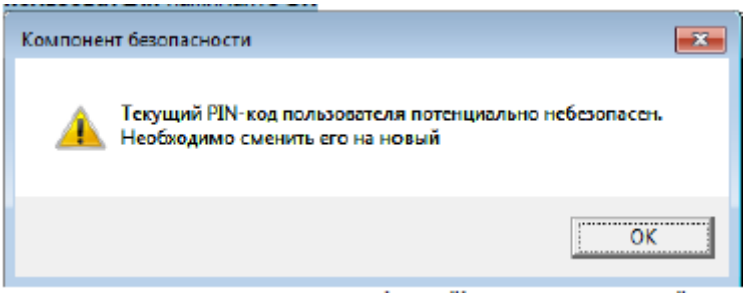


Рисунок 5

PIN-код пользователя по умолчанию (старый) **«12345678»** новый PIN-код должен содержать **не менее 6 и не более 8 символов**

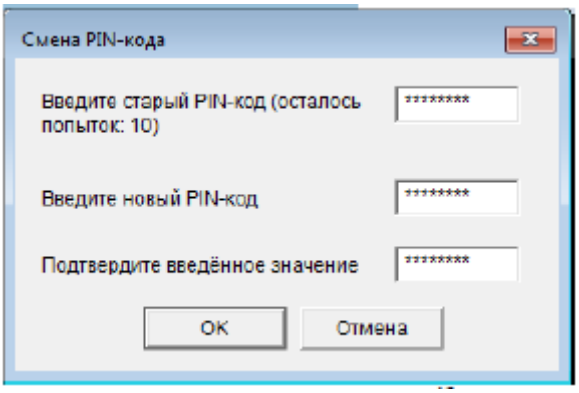


Рисунок 6

Шаг 5.2 Смена PIN-кода Администратора (будет вам необходим в случае блокировки PIN-кода пользователя). PIN-код Администратора по умолчанию (старый) **«87654321»** новый PIN-код должен содержать **не менее 6 и не более 8 символов**

Шаг 5.3 Система попросит ввести PIN-код пользователя (который вы придумали)

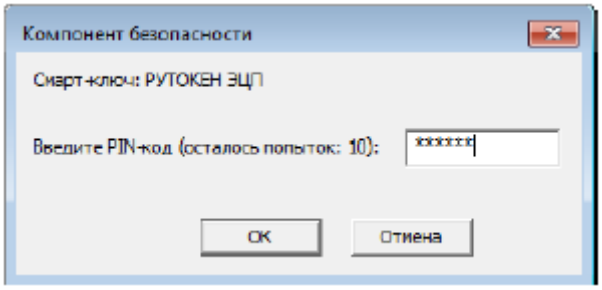


Рисунок 7

Шаг 6. Проверить правильность введенных данных, представленных латинскими буквами. В таком виде данные владельца сертификата хранятся в системе и в самом сертификате (рисунок 15).

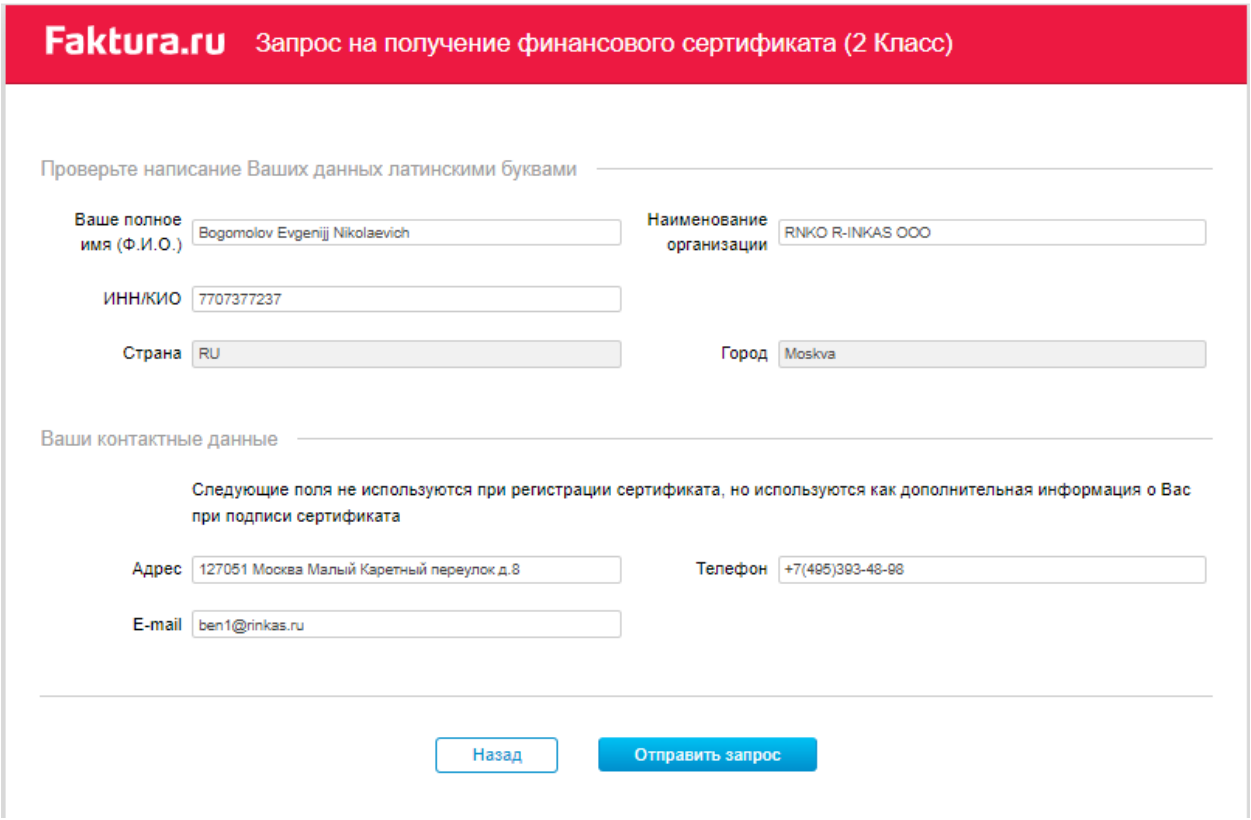


Рисунок 8

Шаг 7. Отправить данные в Удостоверяющий центр: кнопка «Отправить запрос».

Внимание!!! В случае если идентификаторы запроса на сертификат дублируют существующую запись в базе, система сгенерирует ошибку (рисунок 9). Необходимо внести изменения в запрос на сертификат (например, изменить ФИО: добавить символ или заменить имеющийся – Ivanov Ivan Ivanovichh).

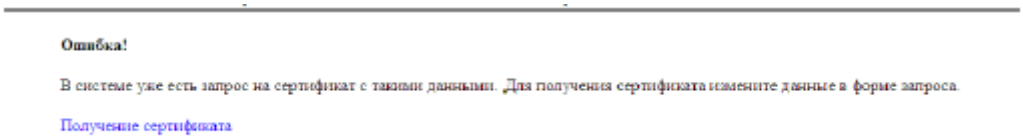


Рисунок 9

Шаг 8. После успешного отправления запроса необходимо перейти по ссылке (рисунок 10) для печати **заявления на получение сертификата для юридических лиц**.

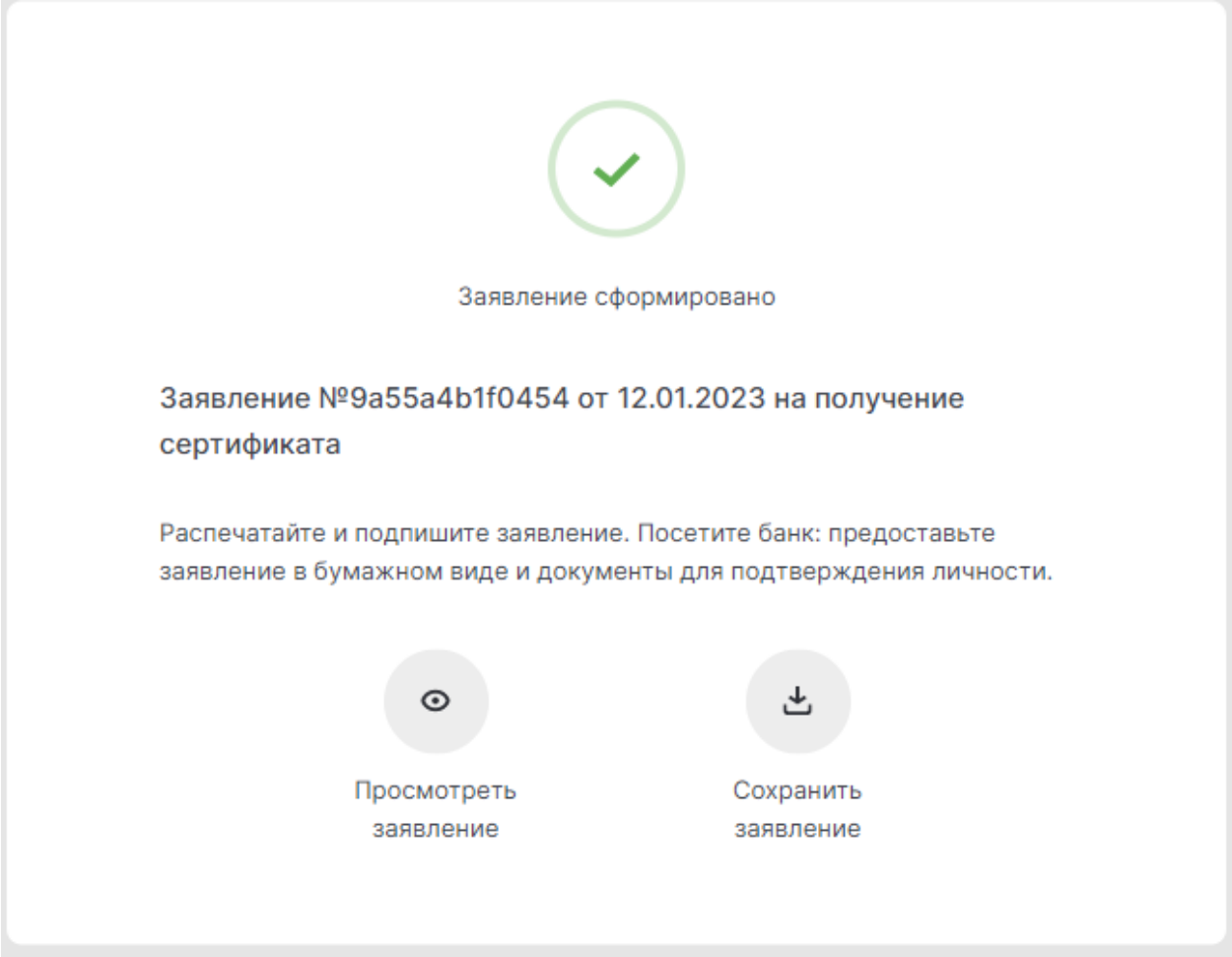


Рисунок 10

Шаг 9. Ввести ФИО заявителя (пользователя сертификата) (рисунок 11 п.1).
Шаг 10. Ввести наименование организации (рисунок 11 п.2).
Шаг 11. Ввести повторно ФИО заявителя (пользователя сертификата) (рисунок 11 п.3).

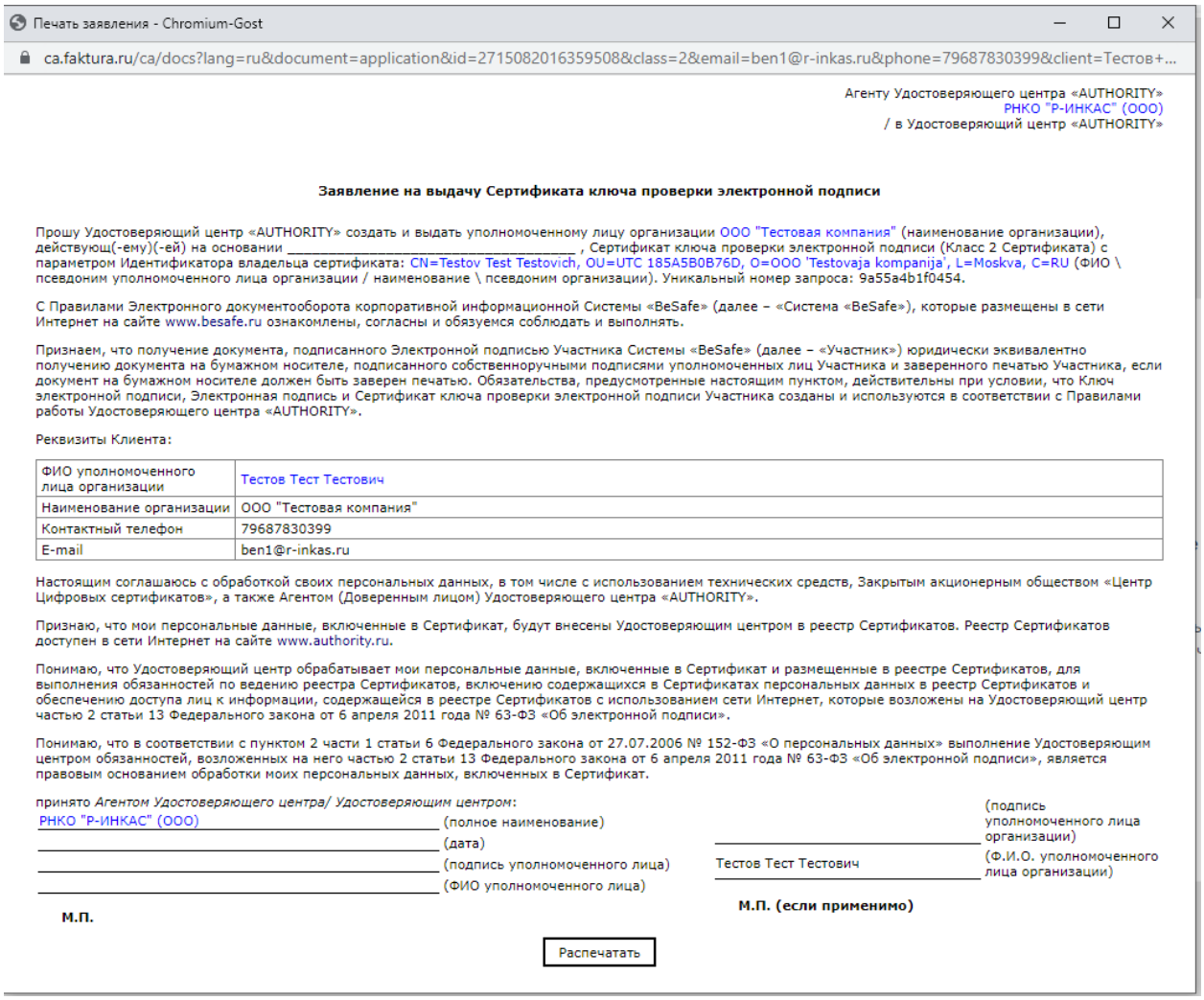


Рисунок 11

Шаг 12. Распечатать заявление в двух экземплярах: кнопка «Распечатать», далее поставить подпись и печать организации. Готовое заявление предоставить операционному работнику Банка. При себе иметь документ, удостоверяющий личность.

Сохранение личного сертификата безопасности на смарт-карту.

Внимание!!! После того, как вы принесете подписанный запроса в Банк, на указанный Вами в запросе на выдачу сертификата электронный адрес придет ссылка (примерное содержимое на рисунке 12).

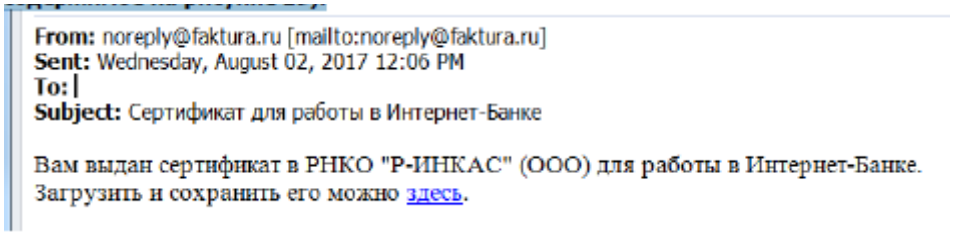


Рисунок 12

Внимание!!! Все нижеописанные действия необходимо выполнять с использованием браузера (интернет-обозревателя) Internet Explorer.

Шаг 1. Перейти по полученной ссылке, кликнув левой кнопкой мыши, либо ввести в адресную строку браузера методом «копировать-вставить».
Шаг 2. Распечатать Акт приема-передачи сертификата открытого ключа, кликнув по ссылке в появившемся окне (рисунок 13).

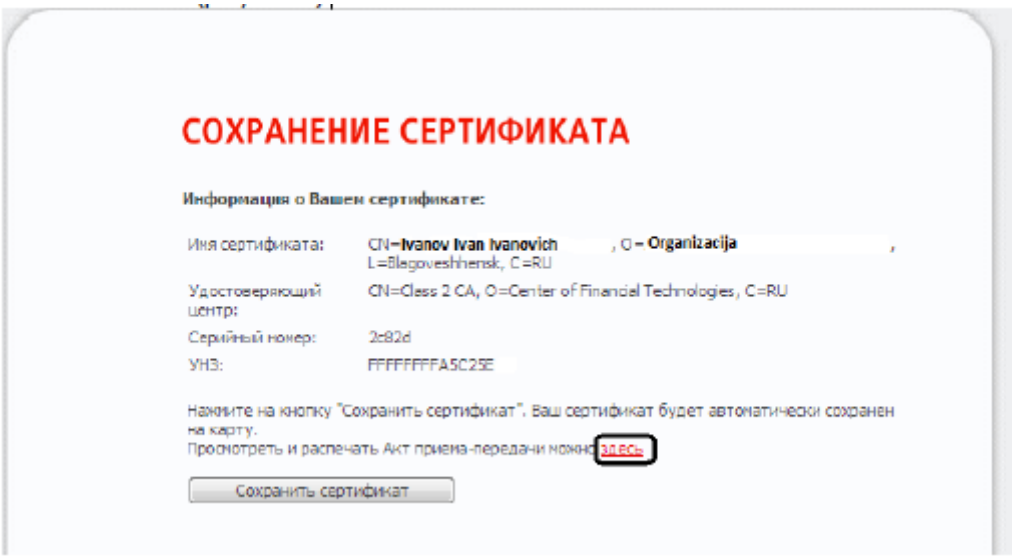


Рисунок 13

Шаг 3. Установить считыватель со смарт-картой в USB-порт рабочей станции (компьютера).
Шаг 4. Сохранить сертификат на смарт-карту: кнопка «Сохранить сертификат». Система предложит ввести PIN-код для доступа к смарт-карте (рисунок 14).

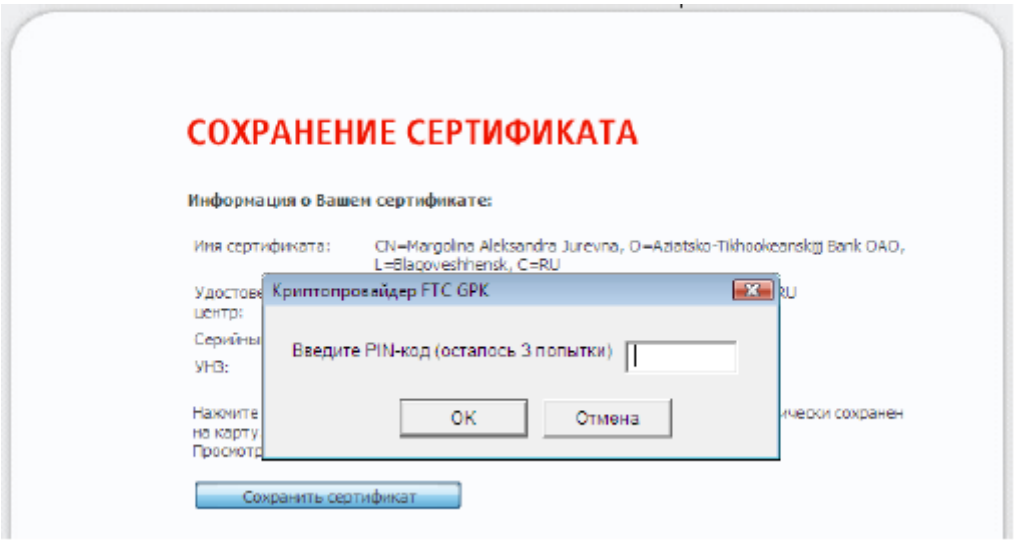


Рисунок 14

Шаг 5. Подтверждаем сохранение сертификата (рисунки 15-16).

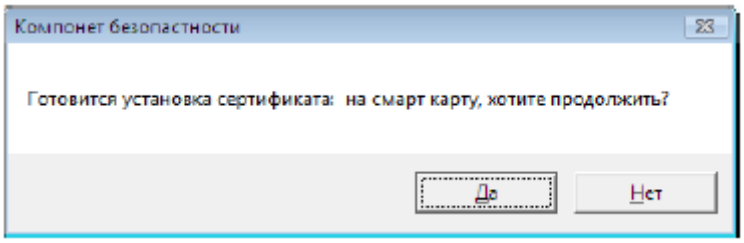


Рисунок 15

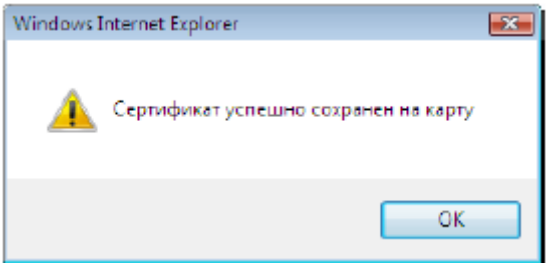


Рисунок 16

Шаг 6. Подписанный Акт приема-передачи сертификата необходимо передать операционному работнику РНКО. На основании данного акта наши сотрудники подключат ваш сертификат (свяжут сертификат и ваш счет).

ВНИМАНИЕ!!! После получения сертификата компьютер готов для работы в системе интернет-банк «Faktura», ярлык для запуска рабочего места находится на рабочем столе.