

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

ВНИМАНИЕ!!! Для браузера Google Chrome, Edge, а также Яндекс.Браузера установите [расширение](#).

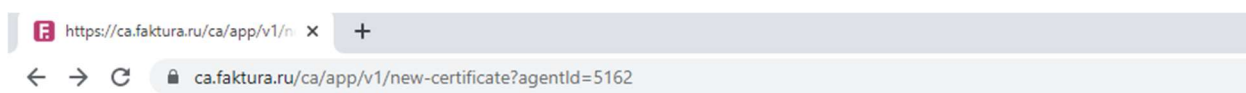
1. Откройте браузер и перейдите по ссылке: <https://business.faktura.ru/f2b/rebus/faq/2.1>
2. Скачайте программное обеспечение для Windows 7, 8, 10.
3. Запустите файл мастера настройки «InternetBankSetup.exe».
4. Следуйте дальнейшим указаниям в окне установки.
5. Нажмите «Завершить» по завершении установки.

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

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>



Удостоверяющий центр "AUTHORITY" (ЗАО "ЦЦС")

English

Получение сертификата

С посещением банка

Подайте заявление в банк лично и получите сертификат:

1. Заполните заявление.
2. Распечатайте и подпишите заявление.
3. Посетите банк, чтобы подтвердить личность и подать заявление в бумажном виде.
4. Сохраните сертификат.

Заполнить заявление

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».

The screenshot shows a web browser window with the URL <https://ca.faktura.ru/ca/app/v1/new-certificate?0&agentId=5162>. The page title is "Заявление на получение сертификата". The form contains the following fields and elements:

- A dropdown menu for "Место хранения сертификата" with "Смарт-ключ (ГОСТ)" selected.
- An information banner: "Убедитесь что смарт-ключ подключен!".
- Input fields for "Фамилия", "Имя", and "Отчество".
- A checked checkbox: "Я получаю сертификат как юридическое лицо".
- An information banner: "Если вы ИП - получайте сертификат физического лица.".
- Input fields for "ИНН / КИО организации", "Наименование организации", and "Документ, на основании которого действую".
- An information banner: "Необходимо указать наименование, номер и дату документа, на основании которого действует уполномоченное лицо (устав, доверенность и тп)".
- Dropdown menus for "Страна" (set to "Россия") and "Город".
- Input fields for "E-mail" and "Телефон".
- An information banner: "На указанный e-mail придёт ссылка для сохранения сертификата и будут приходить уведомления об истечении срока действия сертификата".
- A purple button labeled "Далее" at the bottom right.

Рисунок 1

Шаг 4 При первом обращении к Рутокену система предложит вам сменить **PIN-код** пользователя нажимайте **ОК**

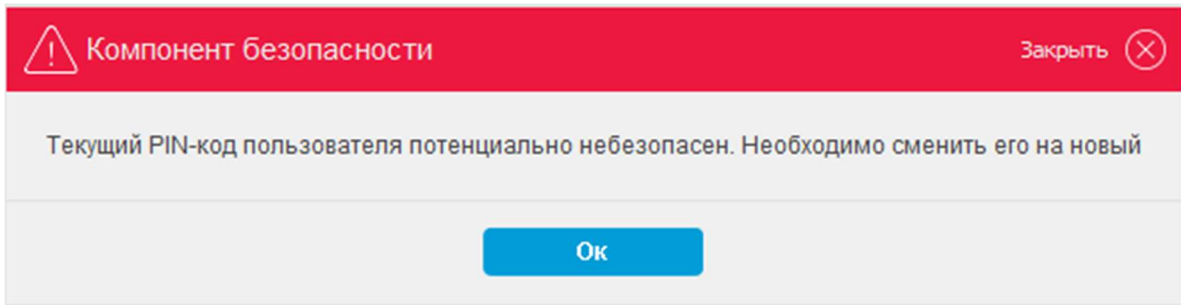


Рисунок 2

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

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

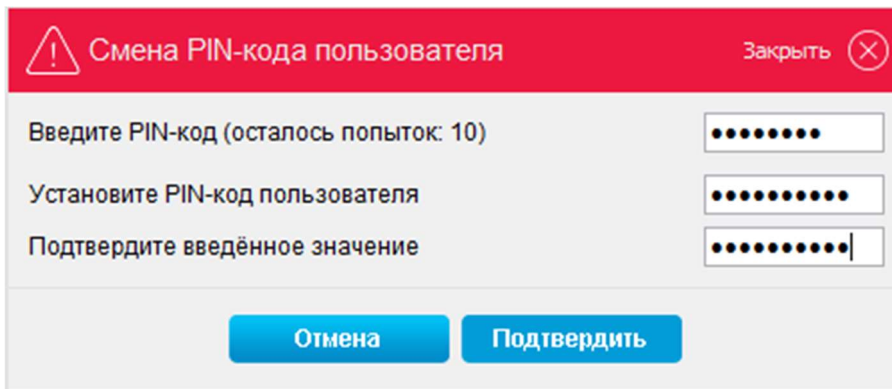


Рисунок 3

Шаг 4.1 Смена PIN-кода Администратора (будет вам необходим в случае блокировки PIN-кода пользователя). PIN-код Администратора по умолчанию «87654321» новый PIN-код должен содержать **не менее 6 и не более 8 символов**

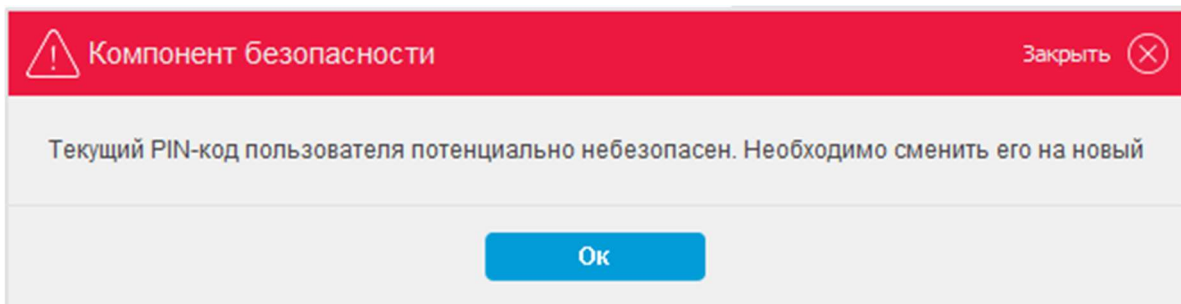


Рисунок 4

The dialog box has a red header with a warning icon and the text "Смена PIN-кода администратора" and a "Закреть" button with a close icon. The main area contains three input fields: "Введите PIN-код администратора (осталось попыток: 10)", "Установите PIN-код администратора", and "Подтвердите введённое значение". At the bottom are two buttons: "Отмена" and "Подтвердить".

Рисунок 5

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

The dialog box has a red header with a warning icon and the text "Компонент безопасности" and a "Закреть" button with a close icon. The main area contains the text "Смарт-ключ: РУТОКЕН ЭЦП" and an input field "Введите PIN-код пользователя (осталось попыток: 7)". At the bottom are two buttons: "Отмена" and "Подтвердить".

Рисунок 6

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

The form has a red header with the logo "Faktura.ru" and the text "Запрос на получение финансового сертификата (2 Класс)". Below the header is a section "Проверьте написание Ваших данных латинскими буквами" with several input fields: "Ваше полное имя (Ф.И.О.)" (Bogomolov Evgenij Nikolaevich), "Наименование организации" (RNKO R-INKAS OOO), "ИНН/КНО" (7707377237), "Страна" (RU), and "Город" (Moskva). Below this is a section "Ваши контактные данные" with a note: "Следующие поля не используются при регистрации сертификата, но используются как дополнительная информация о Вас при подписи сертификата". It contains input fields for "Адрес" (127051 Москва Малый Каретный переулок д.8), "Телефон" (+7(495)393-48-88), and "E-mail" (ben1@rinkas.ru). At the bottom are two buttons: "Назад" and "Отправить запрос".

Рисунок 7

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).

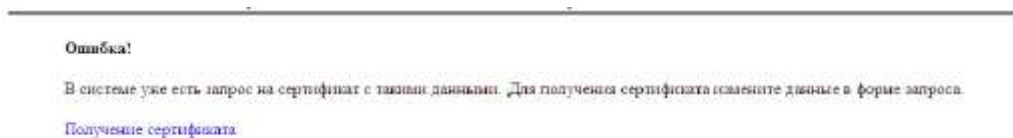


Рисунок 8

Шаг 8. После успешного отправления запроса необходимо перейти по ссылке (рисунок 9) для печати заявления на получение сертификата для юридических лиц.

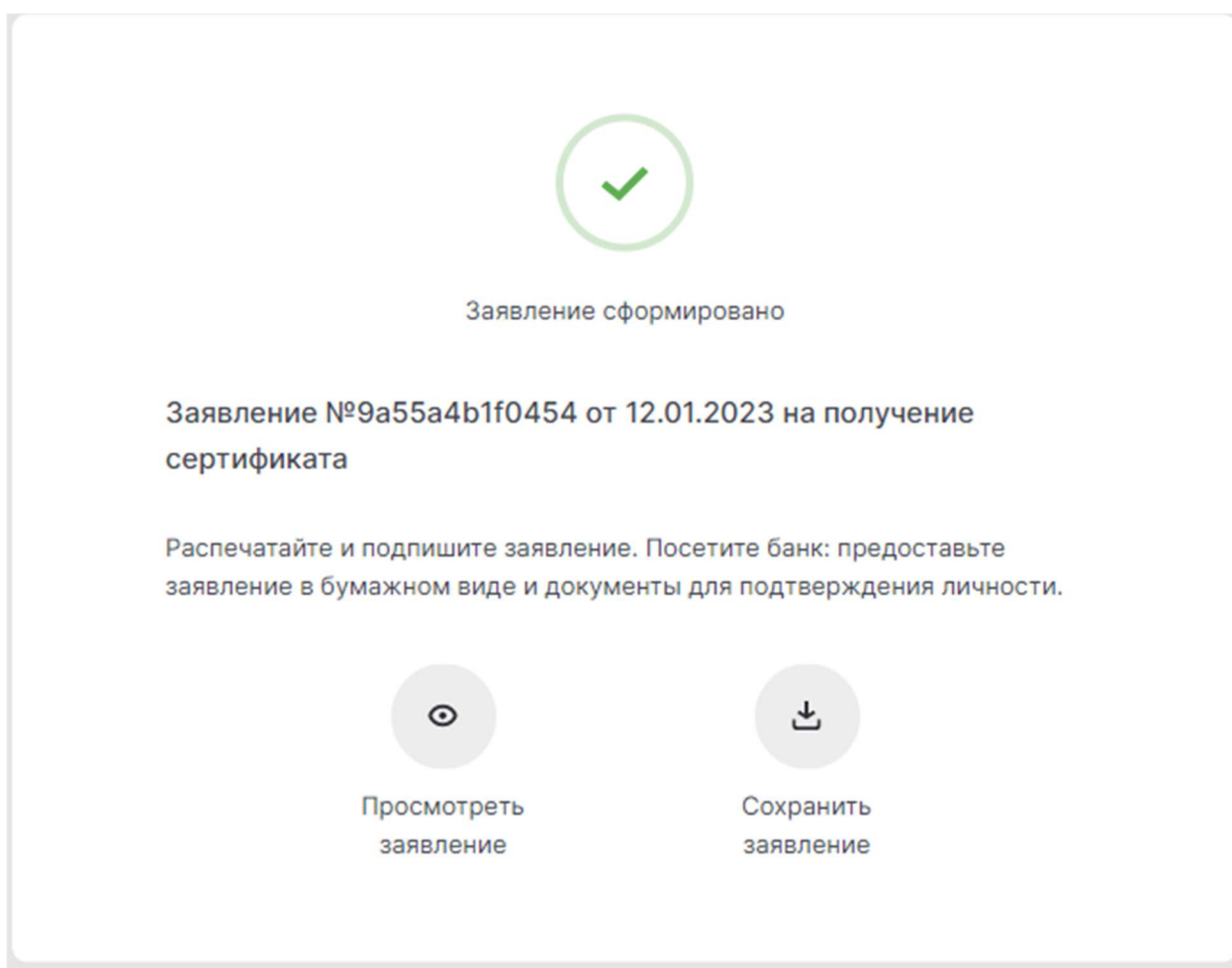


Рисунок 9

Шаг 9. Ввести ФИО заявителя (пользователя сертификата) (рисунок 10 п.1).

Шаг 10. Ввести наименование организации (рисунок 10 п.2).

Шаг 11. Ввести повторно ФИО заявителя (пользователя сертификата) (рисунок 10 п.3).

Печать заявления - Chromium-Gost

ca.faktura.ru/ca/docs?lang=ru&document=application&id=2715082016359508&class=2&email=ben1@r-inkas.ru&phone=79687830399&client=Тестов+...

Агенту Удостоверяющего центра «AUTHORITY»
РНКО "Р-ИНКАС" (ООО)
/ в Удостоверяющий центр «AUTHORITY»

Заявление на выдачу Сертификата ключа проверки электронной подписи

Прошу Удостоверяющий центр «AUTHORITY» создать и выдать уполномоченному лицу организации ООО "Тестовая компания" (наименование организации), действующей(-ему)(-ей) на основании _____, Сертификат ключа проверки электронной подписи (Класс 2 Сертификата) с параметром Идентификатора владельца сертификата: CN=Testov Test Testovich, OU=UTC 185A5B0B76D, O=ООО "Тестовая компания", L=Moskva, C=RU (ФИО \ псевдоним уполномоченного лица организации / наименование \ псевдоним организации). Уникальный номер запроса: 9a55a4b1f0454.

С Правилами Электронного документооборота корпоративной информационной Системы «BeSafe» (далее – «Система «BeSafe»»), которые размещены в сети Интернет на сайте www.besafe.ru ознакомлены, согласны и обязуемся соблюдать и выполнять.

Признаем, 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, предусмотренные 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 уполномоченного лица организации	Тестов Тест Тестович
Наименование организации	ООО "Тестовая компания"
Контактный телефон	79687830399
E-mail	ben1@r-inkas.ru

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».

Признаю, 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, включению 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.

принято Агентом Удостоверяющего центра/ Удостоверяющим центром:
 _____ (подпись уполномоченного лица организации)
 _____ (дата)
 _____ (подпись уполномоченного лица)
 _____ (ФИО уполномоченного лица)

Тестов Тест Тестович (Ф.И.О. уполномоченного лица организации)

М.П. (если применимо)

Рисунок 10

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 11).

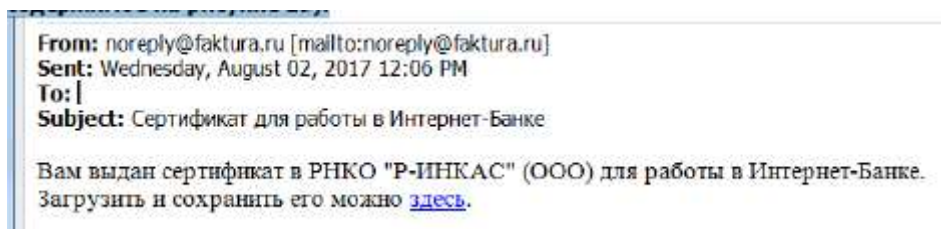


Рисунок 11

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 12).

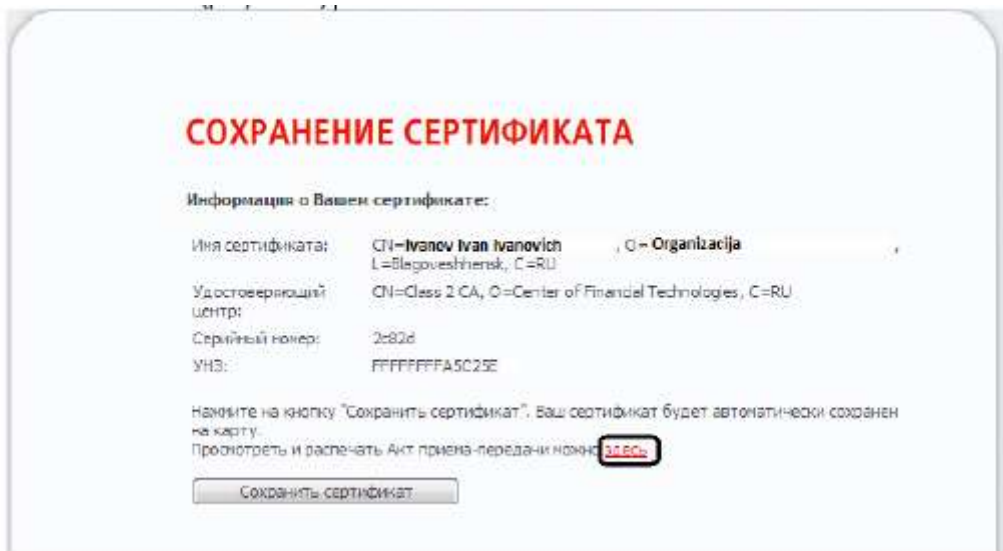


Рисунок 12

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 13).

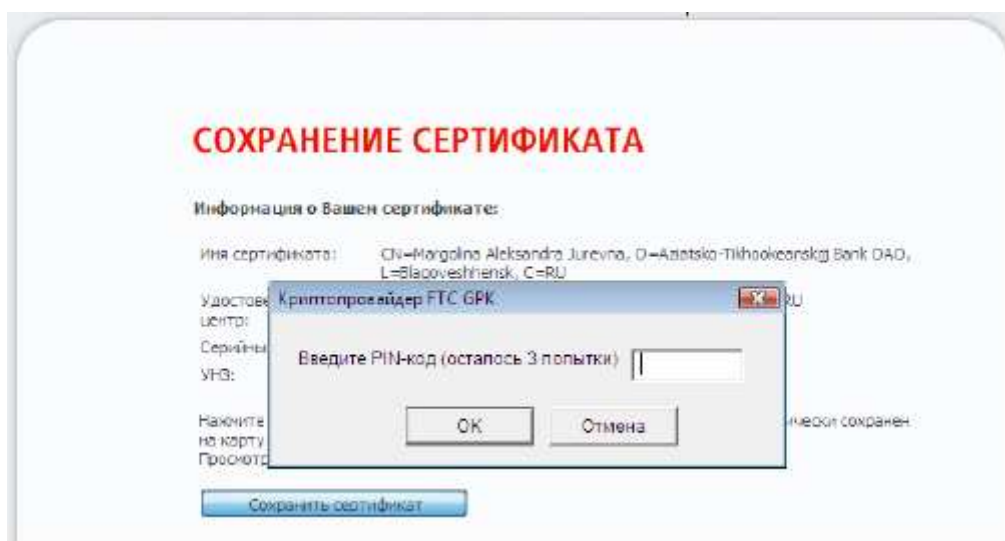


Рисунок 13

Шаг 5. Подтверждаем сохранение сертификата (рисунки 14-15).

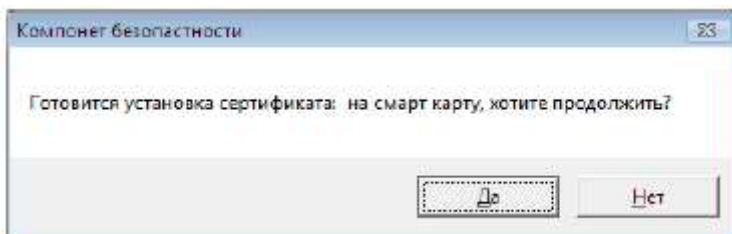


Рисунок 14

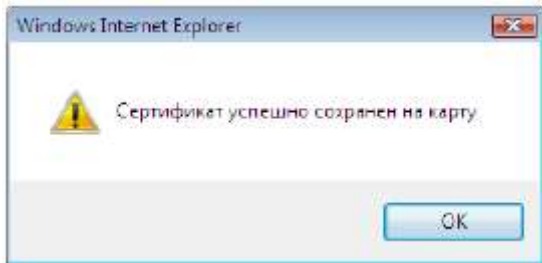


Рисунок 15

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.