РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОЙ РАБОТЕ С СИСТЕМОЙ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ДЛЯ ФИЗИЧЕСКИХ ЛИЦ «IBANK 2»

Для обеспечения безопасности работы в системе дистанционного банковского обслуживания для физических лиц «iBank 2» (далее – Система) применяются:

- шифрование канала связи с использованием протокола TLS и сертификата, подписанного удостоверяющим центром Thawte;
- аутентификация в Системе по учетным данным (логин\пароль);
- разовые коды доступа (подтверждения), рассылаемые при помощи SMS-сообщений;
- рассылка уведомлений об операциях при помощи SMS-сообщений (вход, ошибки аутентификации и т.д.).

ООО ПИР Банк (далее – Банк) информирует о необходимости использования клиентами следующих мер при работе с системой «iBank 2» для повышения безопасности:

При организации рабочего места для работы с системой «iBank 2»

- По возможности, для доступа в Систему Вам необходимо использовать выделенный компьютер с целью минимизации (исключения) возможности его заражения вирусными программами. На компьютере должно быть установлено лицензионное программное обеспечение. Компьютер должен использоваться исключительно для работы в Системе.
- Старайтесь не работать с недоверенных компьютеров (интернет-кафе, киоски и т.д.). При использовании недоверенных компьютеров значительно возрастает риск кражи ваших учетных данных (логина/пароля). При утере мобильного (сотового) телефона с номером (SIM-картой) или отдельно SIM-карты, на номер которой посредством SMS-сообщений Вам направляются коды доступа (подтверждения), возрастает риск несанкционированного использования Ваших учетных данных и кодов доступа (подтверждений).
- Не оставляйте компьютер и мобильное устройство (мобильный телефон, планшетный компьютер) с активной Системой без присмотра. Выходите из Системы, даже если необходимо отойти на непродолжительное время, не оставляйте мобильный телефон с номером (SIM-картой) или отдельно SIM-карту, на номер которой посредством SMS-сообщения Вам направляются коды (доступа) подтверждения без присмотра. Ограничьте доступ посторонних лиц к компьютеру и мобильному устройству (мобильный телефон, планшетный компьютер), с которого Вы осуществляете работу с Системой.
- Убедитесь, что Ваш компьютер не заражен вирусами. Установите и активизируйте антивирусное программное обеспечение. Регулярно обновляйте антивирусные базы. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Вашем логине и пароле.
- Установите и настройте персональный межсетевой экран (брандмауэр, Firewall) на Вашем компьютере, это позволит предотвратить несанкционированный доступ к информации на Вашем компьютере.
- Используйте лицензионное программное обеспечение из проверенных и надежных источников. Выполняйте регулярные обновления операционной системы и

прикладного программного обеспечения (браузер, программы для работы с документами и т.д.).
- При наличии технической возможности включите на Вашем мобильном устройстве режим установки только подписанных приложений с проверкой сертификата и установите антивирусное программное обеспечение.

При использовании парольной защиты и разовых кодов доступа (подтверждения):

- не передавайте никому свои логин и/или пароль и/или код доступа (подтверждения) и/или SIM-карту. При первом входе в Систему необходимо изменить Ваш пароль, воспользовавшись соответствующим разделом Системы.
- не записывайте логин и пароль к Системе там, где доступ к нему могут получить посторонние (включая мобильный телефон и компьютер).
- не храните на мобильном устройстве информацию о доступе к Системе (логин, пароль).
- необходимо вводить только один код доступа (подтверждения), который направляется посредством SMS-сообщения на Ваш зарегистрированный в Банке номер мобильного телефона.

Обращаем Ваше внимание! Не следует реагировать на подозрительные электронные письма и SMS-сообщения, которые запрашивают у Вас конфиденциальную информацию. ООО ПИР Банк не направляет своим клиентам электронные письма и SMS-сообщения (за исключением деловой переписки, инициированной обращением клиента по вопросам, связанным с функционированием Системы). Будьте бдительны: не отвечайте на подобные запросы. В случае получения такого сообщения просим Вас незамедлительно сообщить об этом по телефонам Банка.

При формировании пароля предлагается соблюдать следующие правила:
- рекомендуемая длина пароля должна быть не менее 8 символов;
- рекомендуется использовать латинские буквы, набранные в разных регистрах (a-z, A-Z, a-Z), цифры и специальные символы (@, #, $, &, *, % и т.п.);
- при смене пароля для входа в Систему новое значение должно отличаться от предыдущего не менее чем на 3 символа;
- новое значение пароля для входа в Систему не должно совпадать с предыдущими паролями на протяжении четырех смен;
- пароль не должен основываться на информации, которую другие могут легко угадать или узнать (имена, номера телефонов, даты рождения, идентификаторы пользователей, наименования рабочих станций и т.п.);
- пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.);
- пароль не должен являться словарным словом (например, «password» - это ненадежный пароль);
- пароль не должен являться копией других паролей пользователя, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете);
- пароль не должен содержать последовательность одинаковых символов и групп символов (например, не должны применяться пароли, состоящие из одинаковых цифр или из одинаковых букв);
- периодически производите замену пароля для входа в Систему, ни при каких условиях не сообщайте информацию о Вашем пароле никому, включая сотрудников Банка, родственников и иных третьих лиц;
- не сохраняйте информацию о Вашем пароле на вход в Систему на любых

носителях, включая компьютер.

При использовании системы «iBank 2»:

- Проверяйте, что соединение действительно происходит в защищенном режиме TLS, при этом веб-браузер должен показывать значок закрытого замка (Примеры для проверки приведены в Приложении 1).
- Проверяйте, что соединение установлено именно с сервером системы «iBank 2» именно по адресу **https://ibank.pirbank.ru/web_banking** Во избежание попыток неправомерного получения персональной информации рекомендуется вводить указанный адрес вручную. Убедитесь, что информация о сертификате сайта соответствует URL **https://ibank.pirbank.ru/web_banking** (Примеры для проверки приведены в Приложении 1).
- Помните, что сайты, визуально напоминающие банковский сайт, создаются специально для незаконного получения Вашей персональной информации. В случае обнаружения сайта копирующего дизайн корпоративного сайта ООО ПИР Банк или системы «iBank 2» просим Вас незамедлительно сообщить об этом по телефонам Банка: **+7 (495) 691-69-32.**
- Проверьте, что сертификат сайта выдан удостоверяющим центром THAWTE. Для этого, откройте информацию о сертификате и убедитесь, что издателем (кем выдан) является «Thawte Extended Validation SSL CA – G3» (Примеры для проверки приведены в Приложении 1).
- Проверяйте информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему.
- При запросе окна браузера об использовании автозаполнения полей формы (логина и пароля) откажитесь от данной функции.
- Обращайте внимание на изменения привычных Вам страниц входа в Систему или подтверждения операции. Любые изменения, особенно касающиеся безопасности, обязательно заранее анонсируются в новостях Системы или на сайте Банка. Если вы сомневаетесь, действительно ли содержимое страницы вы получаете с сервера Банка, а не от компьютерного вируса, обязательно позвоните в Банк или попробуйте открыть ту же страницу Системы на другом компьютере, подключенном к другой сети. БАНК ВСЕГДА ПРЕДУПРЕЖДАЕТ ОБО ВСЕХ ИЗМЕНЕНИЯХ, ПРОИЗВОДИМЫХ В СИСТЕМЕ. НИКОГДА НЕ ПОЛЬЗУЙТЕСЬ ИНТЕРФЕЙСОМ, ИЗМЕНЕНИЕ КОТОРОГО НЕ ПОДТВЕРЖДЕНО БАНКОМ.
- Заходите в Систему не реже одного раза в 14 (четырнадцать) календарных дней, в том числе для ознакомления с информацией, размещаемой Банком, и касающейся работы в Системе.
- Не отвечайте на подозрительные письма с просьбой выслать, логин\пароль, одноразовый код доступа (подтверждения), номер карты и другие конфиденциальные данные. Не стоит также сообщать свои конфиденциальные данные и сотрудникам Банка, поскольку их не должен знать никто, кроме Вас.
- При регистрации в Системе не следует указывать (изменении номера мобильного телефона для SMS-сообщений) номера не принадлежащих Вам телефонов. На указанные номера будут приходить SMS-сообщения с одноразовым кодом для доступа (подтверждения) операций в Системе. Во избежание несанкционированных операций в Системе не следует передавать телефоны, номера которых зарегистрированы в Системе, посторонним.
- Рекомендуется установить пароль на доступ к телефону и/или на доступ к SMS-сообщениям.
- Не оставляйте без присмотра Ваш мобильный телефон с номером (SIM-картой) или

отдельно SIM-карту, на номер которой посредством SMS-сообщения Вам направляются коды доступа (подтверждения).

- Не рекомендуется передача телефонного аппарата или SIM-карты другим лицам, т.к. на оставленном без присмотра телефоне может быть совершен ряд действий направленных на получение доступа к Системе, например, злоумышленник может установить вредоносное программное обеспечение, настроить переадресацию SMS-сообщений на другой телефонный аппарат и т.п.
- Не рекомендуется загружать и устанавливать на телефонный аппарат программное обеспечение, полученное из подозрительного источника: интернет-сайты, ссылки в SMS и MMS-сообщениях.
- Следует осуществлять информационное взаимодействие с Банком только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в Банке.
- **Внимательно контролируйте все операции, совершенные в Системе.**
- После окончания работы в Системе обязательно закройте окно Системы с помощью кнопки «Выход».

При возникновении кризисных ситуаций

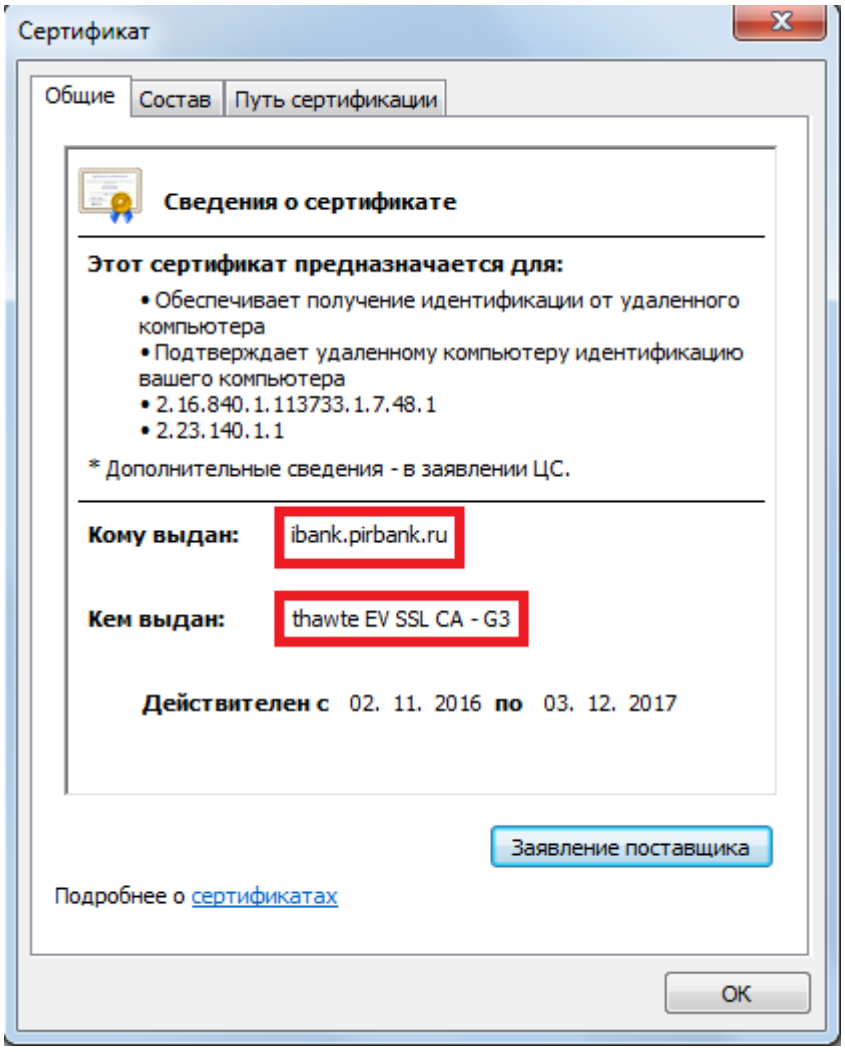
- В случае возникновения подозрений на мошеннические действия:
  - В Системе присутствуют действия, которые Вы не совершали;
  - Подозрительная активность на компьютере, с которого осуществляется работа с Системой (самопроизвольные движения мышью, открытие/закрытие окон, набор текста и т.п.);
  - Изменения адреса для соединения с Системой;
  - Изменения IP-адреса, с которого осуществлялось подключение к Системе (изменилась сеть);
  - Невозможности получения доступа к Системе по причине несовпадения логина или пароля на вход в Систему;
  - Изменение интерфейса Системы;
  - Внезапное приостановление работы SIM-карты (блокировка SIM-карты). Возможно незаконное изготовление 3-ми лицами дубликата Вашей SIM-карты (необходимо обратиться к Вашему оператору мобильной связи);
  - Подозрительная работа мобильного устройства (мобильный телефон, планшетный компьютер), с которого осуществляется работа с Системой. Возможно заражение мобильного устройства вредоносным программным обеспечением.
- или при возникновении опасений, что Ваш логин или пароль стал известен посторонним необходимо выполнить следующие действия:
  - Выйдите из Системы;
  - Заблокируйте технические средства (в том числе, выключите компьютер), используемые для работы в Системе;
  - При появлении подозрений, что Ваши логин и/или пароль стали известны третьим лицам, SIM-карта стала доступна третьим лицам, незамедлительно блокируйте доступ в Систему по телефонам Банка (с последующим оформлением в Банке соответствующего письменного заявления), либо обратившись в отделение Банка;
  - В случае утраты логина и/или пароля незамедлительно блокируйте доступ в Систему, обратившись по телефонам Банка (с последующим оформлением в Банке соответствующего письменного заявления), либо посетив отделение

Банка;
  - В случае утери телефонного аппарата и/или SIM-карты незамедлительно обратитесь в Банк для блокировки доступа к Системе по телефонам Банка (с последующим оформлением в Банке соответствующего письменного заявления) или обратившись в отделение Банка;
  - При оформлении письменного заявления о блокировке Системы обязательно опишите обстоятельства компрометации логина, пароля, кодов (доступа) подтверждения или несанкционированного доступа, либо другую информацию по фактам, вызвавшим Ваши подозрения.
- **Смена номера телефона, возможна только по заявлению, оформленному в отделении Банка.**
- Возобновление доступа в Системе производится в офисе Банка при Вашем личном обращении.

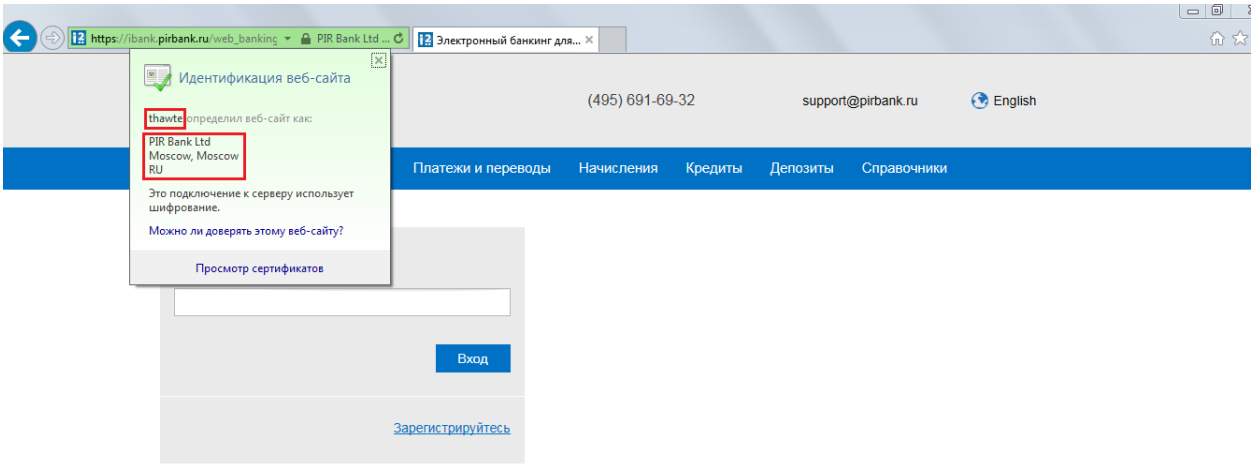
Банк обращает Ваше внимание на то, что выполнение вышеописанных рекомендаций позволит существенно снизить риски несанкционированного использования системы «iBank 2».

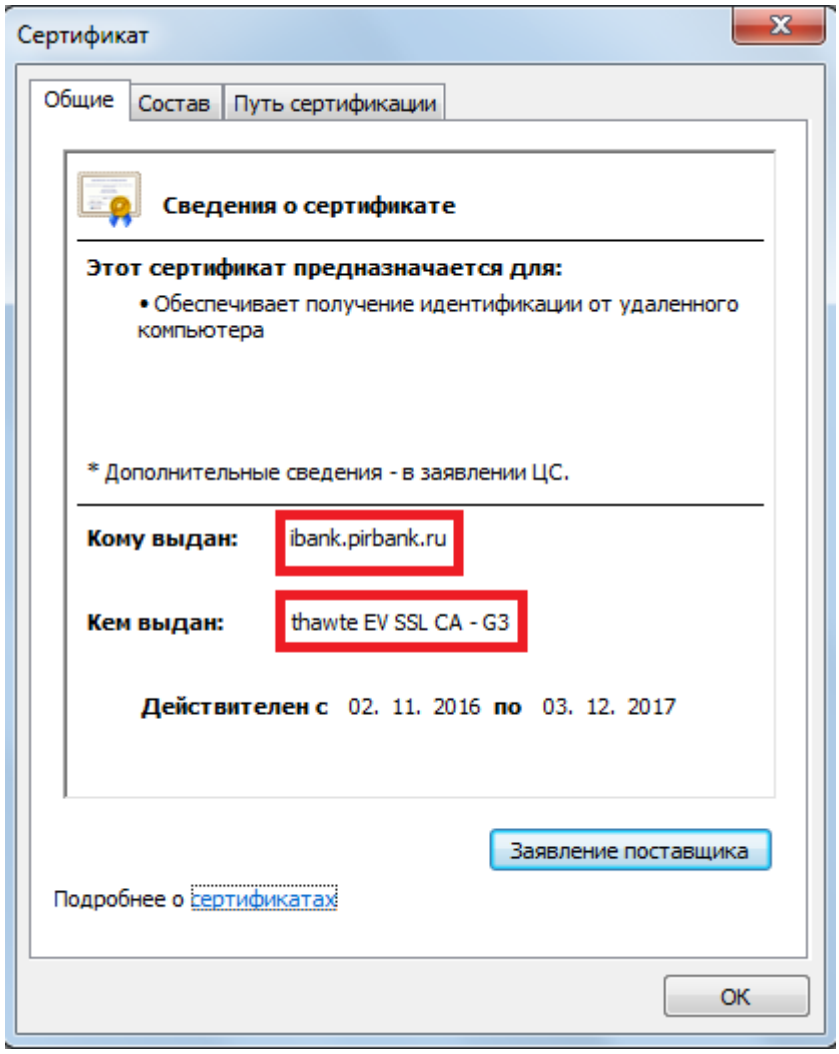
Приложение 1
к Рекомендации по безопасной работе с системой дистанционного банковского обслуживания для физических лиц «iBank 2» ООО ПИР Банк

Сведения о сертификате системы «iBank 2»

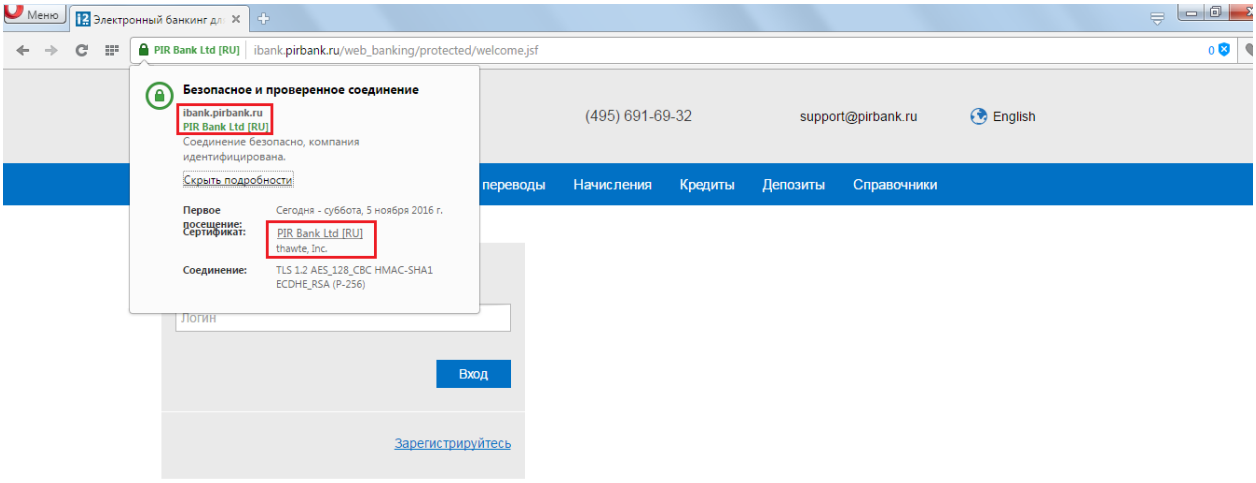


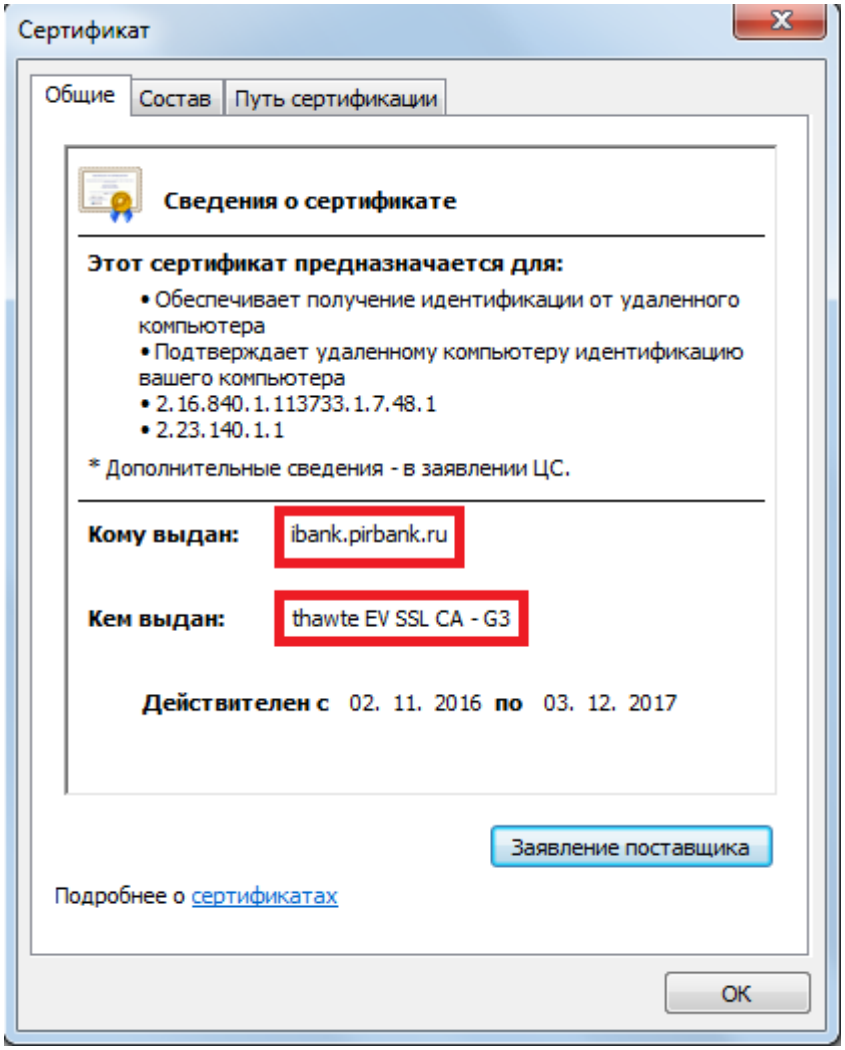
При работе с браузером Internet Explorer





При работе с браузером Opera





При работе с браузером Mozilla Firefox