



Руководство пользователя
по Системе «Интернет-банк»

1. Общая информация

Руководство пользователя по Системе «Интернет-банк» (далее – Руководство пользователя) разработано для пользователей данной Системы и находится в свободном доступе для всех Клиентов Банка на Официальном сайте Банка и/или Системы.

Иные термины, используемые в настоящем Руководстве пользователя, имеют то же значение, что и в Условиях.

Для работы с Системой «Интернет-банк» необходимо быть Клиентом Банка, либо стать Клиентом Банка с соблюдением норм действующего законодательства по идентификации физических лиц.

Действующим Клиентам в процессе регистрации/восстановления в Системе необходимо указать номер действующей Карты и данные документа, удостоверяющего личность, либо воспользоваться процессом входа через Единый портал государственных услуг (при наличии технической возможности).

Новым Клиентам можно обратиться в ближайший офис Банка для получения Карты, который обслуживает физических лиц или подать заявку на Официальном сайте Банка, при этом такая Карта может быть доставлена курьером. Также доступен вариант регистрации в качестве Клиента Банка с использованием Единой биометрической системы (пункт меню «Стать клиентом») на Официальном сайте Банка и/или Системы, такой процесс сопровождается, в том числе, и регистрацией Клиента в Системе.

Для входа в Систему необходимы Идентификатор пользователя (логин) и Пароль (подробнее см. пункт 2 «Получение доступа»).

Для проведения некоторых операций через Систему необходимо использование Разового кода безопасности (подробнее см. пункт 3 «Разовый код»).

Для использования Системы необходимо зайти на сайт <https://my.bank-hlynov.ru>, и/или установить Мобильное приложение «Банк Хлынов», после чего ввести Идентификатор пользователя (логин) и Пароль (подробнее см. пункт 6 «Регистрация в Системе»).

В случае возникновения каких-либо вопросов по регистрации и работе в Системе «Интернет-банка» или получения другой консультации, достаточно перейти в окно Чата в нижнем правом углу страницы Сайта (вкладка «Чат» в Приложении) и задать интересующий вопрос (подробнее см. пункт 13 «Чат»).

В случае необходимости оперативная блокировка/разблокировка доступа к Системе «Интернет-банк» осуществляется через Единый Сервисный центр Банка по телефону 8 (800) 250-2-777 (звонок по России бесплатный).

Обратите внимание, что все, используемые в Руководстве пользователя данные, являются обезличенными и не имеют отношения к какому-либо реальному физическому лицу.

2. Получение доступа

2.1 При наличии действующей Карты в Банке вы можете получить доступ к Системе следующими способами:

- 1) Зарегистрироваться самостоятельно на Официальном сайте Системы или с помощью Мобильного приложения;
- 2) Обратиться в любой офис Банка;
- 3) Зарегистрироваться с помощью устройства самообслуживания «Все просто!».

При подключении к Системе в офисе Банка или через устройство самообслуживания «Все просто!», Логин и Транспортный пароль отправляется в SMS-сообщении на ваш Номер мобильного телефона. При первом входе в Систему необходимо изменить Транспортный пароль на Постоянный. Также рекомендуем Вам изменить Логин. (Подробнее см. пункт 8 «Изменение логина и пароля»).

2.2 При отсутствии действующей Карты в Банке, но являясь Клиентом, вы можете получить доступ к Системе таким способом (при наличии технической возможности, доступности пункта меню или визуального элемента интерфейса):

- выбрать соответствующий пункт меню Системы, близкий по смыслу «Вход через Госуслуги». Войти в свой Личный кабинет на Едином портале государственных услуг и дать Банку разрешения, которые позволят предоставить доступ к Системе.

При прохождении регистрации на Официальном сайте Системы или Мобильном приложении, необходимо самостоятельно установить Логин и Пароль. (См. пункт 6 «Регистрация в Системе»).

2.3 При отсутствии действующих договоров с Банком Вы можете получить доступ к Системе одним из способов:

- 1) Зарегистрироваться самостоятельно на Официальном сайт Банка или Мобильном приложении Банка с использованием Единой биометрической системы (при наличии технической возможности, доступности пункта меню или визуального элемента интерфейса);
- 2) Подписать необходимый пакет документов в личном кабинете на сайте или в мобильном приложении Финансовой платформы.

3. Разовый код безопасности

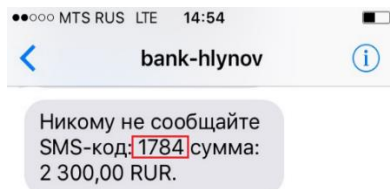
Разовый код безопасности используется для дополнительной Аутентификации пользователя при совершении операций в Системе:

Обратите внимание! Банк по своему усмотрению определяет комплекс мер для повышения уровня безопасности при использовании Системы Клиентом и определяет случаи, когда использование Разового кода безопасности необходимо. В каждый конкретный момент происходит оценка Клиента, действий Клиента и принимается решение о необходимости запросить с Клиента ввод Разового кода безопасности.

Разовый код безопасности отправляется Банком посредством SMS-сообщения в процессе выполнения операции на Номер мобильного телефона. Разовый код безопасности имеет ограниченное действие и может быть использован только для подтверждения конкретной операции. В каждый момент времени действителен только один Разовый код безопасности. При необходимости, например, код по каким-либо причинам не приходит, Разовый код безопасности можно запросить повторно. Разовый код безопасности приходит от отправителя «bank-hlynov».

Обратите внимание! Никому не сообщайте Разовый код безопасности для подтверждения операций в Системе.

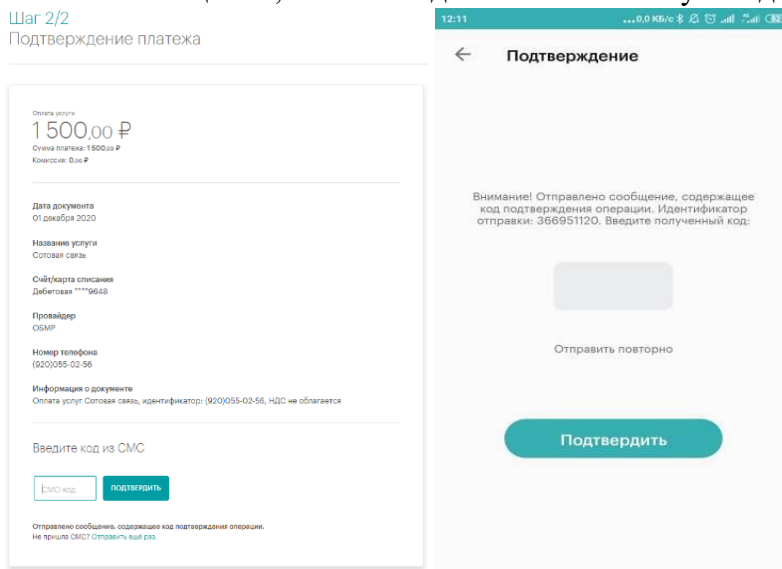
Пример SMS-сообщения с Разовым кодом безопасности:



где **1784** – Разовый код безопасности операции

4. Подтверждение операций Разовым кодом безопасности

Для подтверждения операций по запросу Системы необходимо ввести Разовый код безопасности, который был отправлен в SMS-сообщении, в поле ввода и нажать кнопку «Подтвердить»:

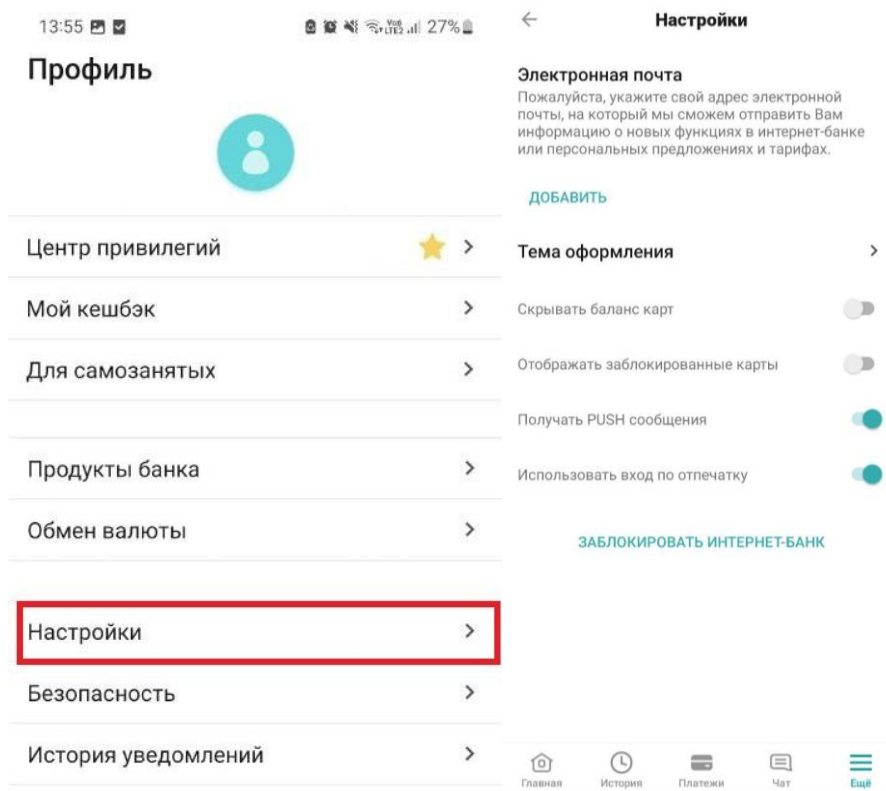


5. Push-уведомление

Банк предлагает услугу уведомления Клиента об операциях и авторизациях по Картам и об операциях, совершаемых в Системе, посредством SMS-сообщений и Push-уведомлений. Такое уведомление производится в зависимости от тарифного плана Карты и выбранной по нему периодичности получения уведомлений и их платности (Подробнее см. «Условия пользования банковскими картами АО КБ "Хлынов", документ доступен на Официальном сайте Банка). Для получения Push-уведомлений Клиенту необходимо наличие подключения Мобильного устройства к мобильной (подвижной радиотелефонной) связи и/или сети Интернет.

5.1. Включение Push-уведомлений

Подключение Push-уведомлений возможно по инициативе Банка при первой установке Мобильного приложения на Мобильное устройство с последующей Аутентификацией Клиента в таком приложении и добавлении Мобильного устройства в список доверенных. Клиент может отключить получение Push-уведомлений через «Настройки» в Мобильном приложении. В случае невозможности доставить Банком Push-уведомления по независящим от Банка обстоятельствам (у Клиента отсутствует доступ к сети Интернет, Мобильное устройство отключено, низкий или нестабильный сигнал мобильной сети и т.д.), Банк направляет SMS-сообщение на Номер телефона Клиента. Push-уведомление отображается на экране Мобильного устройства в виде всплывающего уведомления и может быть впоследствии просмотрено в Мобильном приложении Банка в «Истории уведомлений»



6. Регистрация в Системе, требования безопасности для Логина и Пароля

Обратите внимание! При составлении Логина и Пароля рекомендуем вам пользоваться требованиями безопасности.

Требования безопасности для Логина:

- длина от 6 до 30 символов;
- может состоять из букв латинского алфавита, цифр 0-9 и специальных символов: «@», «_», «-», «.» (иные элементы пунктуации, в том числе пробел, не допустимы);
- регистр букв значения не имеет.

Требования безопасности для Пароля:

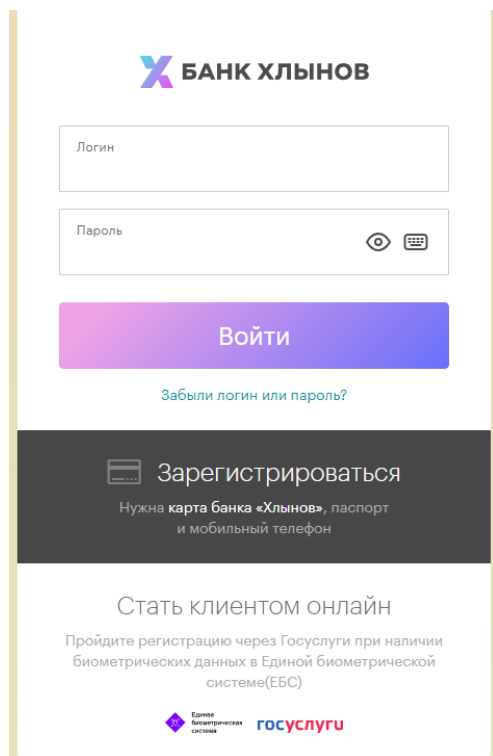
- длина от 8 до 30 символов;
- должен содержать буквы латинского алфавита в разных регистрах и как минимум одну цифру;
- не должен содержать 3 и более одинаковых символов или цифр подряд;
- может содержать элементы пунктуации из списка: «!», «@», «#», «\$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «:», «;», «,», «.» (иные элементы пунктуации, в том числе пробел, не допустимы).

Обратите внимание! Если вы проводите не самостоятельную регистрацию в Системе, указывая при этом с соблюдением требований Логин и Пароль, то первый вход в Систему осуществляется по присвоенным вам Системой Логину и Транспортному паролю. Такие Логин и Транспортный Пароль необходимо сменить после успешного входа в Систему.

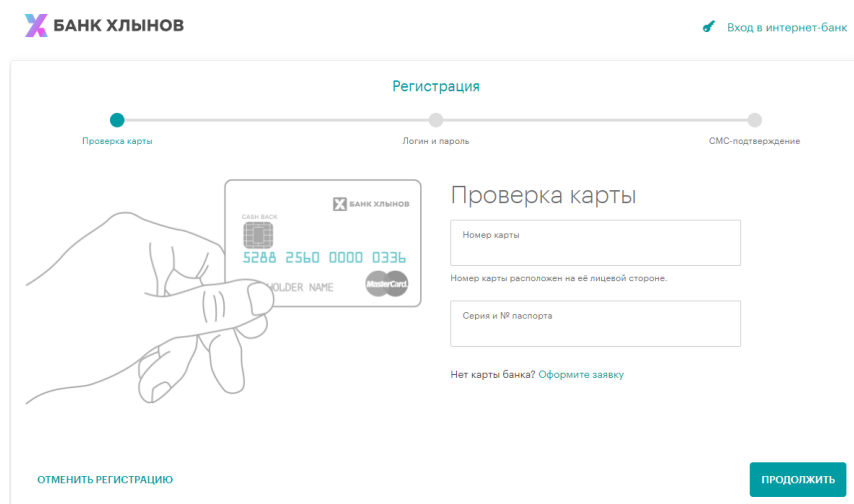
6.1. Регистрация в Системе на Официальном сайте Банка

Вы можете получить доступ к Системе путем регистрации на странице входа в Систему, не выходя из дома. Для этого вам потребуется документ, удостоверяющий личность, действующая Карта Банка и мобильный телефон.

Для регистрации щелкните ссылку «**Зарегистрироваться**» на Странице входа в Систему.



На открывшейся странице необходимо заполнить следующие данные: номер действующей основной Карты, который изображен на ее лицевой стороне (16 цифр), номер документа, удостоверяющего личность.



После ввода номера Карты и реквизитов паспорта необходимо нажать «**Продолжить**».

В появившемся окне «**Создание профиля**» нужно указать желаемые Логин и Пароль (необходимо

повторить ввод Пароля в поле «Повторить пароль»).

После создания Логина и Пароля необходимо ознакомиться с Условиями обслуживания в интернет-банке АО КБ «Хлынов» и отметить пункт «Прошу подключить меня к системе интернет-банк АО КБ «Хлынов»». Ознакомлен и согласен с Условиями обслуживания в интернет-банк АО КБ «Хлынов».

Регистрация

Проверка карты Логин и пароль СМС-подтверждение

Создание профиля

Логин

Пароль

Повторите пароль

Прошу подключить меня к системе интернет-банк АО КБ «Хлынов»
Ознакомлен и согласен с условиями обслуживания в интернет-банке АО КБ «Хлынов»

Логин должен отвечать следующим требованиям:

- длина от 6 до 30 символов;
- состоит из букв латинского алфавита, цифр 0-9 и специальных символов «@», «_», «>», «<»;
- регистр букв значение не имеет.

Пароль должен отвечать следующим требованиям:

- длина от 8 до 30 символов;
- состоит из букв латинского алфавита в разных регистрах и как минимум одной цифры;
- не должен содержать 3 и более одинаковых символов или цифр подряд;
- может содержать элементы пунктуации из списка: «!», «@», «#», «\$», «%», «&», «'», «(», «)», «_», «:», «>», «<», «=», «+», «-», «/», «\», «.»

ОТМЕНИТЬ РЕГИСТРАЦИЮ ПРОДОЛЖИТЬ

При успешной регистрации в Системе по кнопке «Продолжить» необходимо перейти на окончательный этап регистрации «SMS-подтверждение».

Регистрация

Проверка карты Логин и пароль СМС-подтверждение

СМС-подтверждение

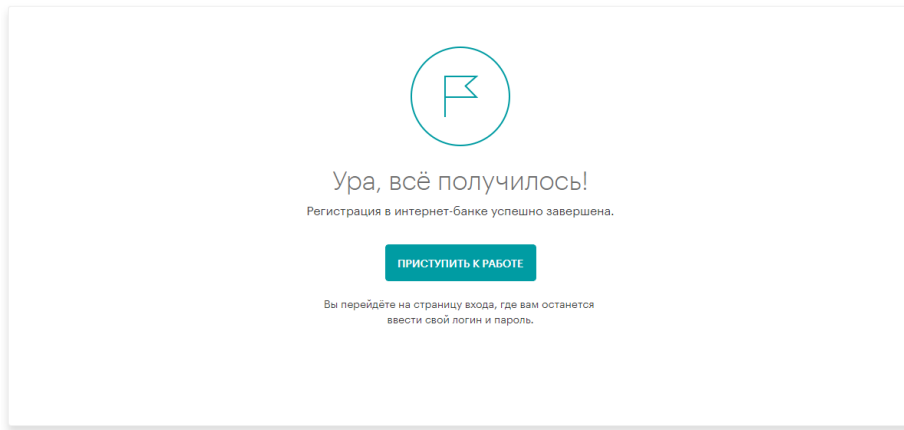
СМС-код

Сейчас Вы получите СМС с кодом идентификации

Не пришла SMS? [Повторить](#)

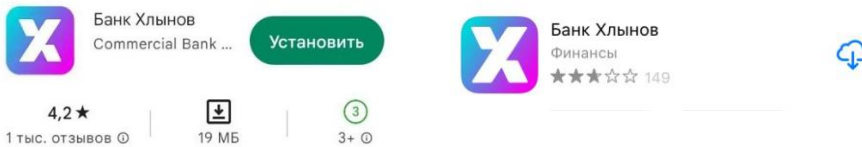
ПРОДОЛЖИТЬ

На привязанный к Карте Номер мобильного телефона придет Разовый код безопасности. После ввода кода из SMS-сообщения регистрация в Системе «Интернет-банк» будет завершена и можно приступить к работе.

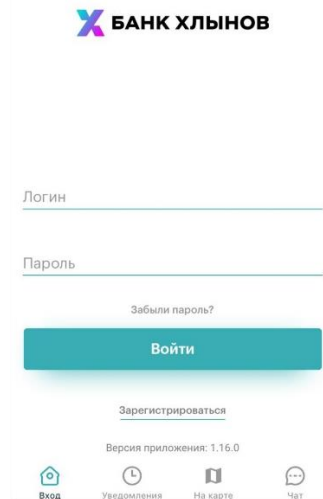


6.2. Регистрация через Мобильное приложение

Для начала работы с мобильной версией Системы необходимо в сервисе Google Play Market, Apple Store, Huawei AppGallery, RuStore скачать на Мобильное устройство Мобильное приложение «**Банк Хлынов**». (Системные требования для корректной работы Приложения: ОС Android 5.0 и выше, iOS 13 и выше)



Для регистрации щелкните ссылку «**Зарегистрироваться**» на открывшейся странице. Для регистрации вам потребуется документ, удостоверяющий личность, действующая основная Карта Банка и мобильный телефон для получения Разового кода безопасности.



На открывшейся странице проверки Карты необходимо заполнить следующие данные: номер действующей основной Карты, который изображен на ее лицевой стороне (16 цифр), номер документа, удостоверяющего личность.

Вход в интернет-банк

Проверка карты

Номер карты

Номер карты расположен на её лицевой стороне.

Серия и № паспорта

Нет карты банка? Оформите заявку

ПРОДОЛЖИТЬ

После ввода номера Карты и реквизитов документа, удостоверяющего личность, продолжить процесс регистрации нажатием на **«Продолжить»**.

В появившемся окне **«Создание профиля»** нужно указать желаемые Логин и Пароль (Пароль необходимо повторно ввести в поле **«Повторить пароль»**).

После создания Логина и Пароля необходимо ознакомиться с Условиями обслуживания в интернет-банке АО КБ «Хлынов» и отметить пункт **«Прошу подключить меня к системе интернет-банк АО КБ «Хлынов»**, ознакомлен и согласен с Условиями обслуживания в интернет-банк АО КБ «Хлынов».

Вход в интернет-банк

Создание профиля

Логин

Пароль

Повторите пароль

Прошу подключить меня к системе интернет-банк АО КБ «Хлынов»

ПРОДОЛЖИТЬ

При успешном создании профиля в Системе по кнопке **Продолжить** осуществить переход на окончательный этап регистрации **«SMS-подтверждение»**.

СМС-подтверждение

СМС-код

Сейчас Вы получите СМС с кодом идентификации

Не пришла SMS? [Повторить](#)

ПРОДОЛЖИТЬ

На привязанный к Карте Номер мобильного телефона придет **Разовый код безопасности**.

После ввода кода из SMS-сообщения регистрация в Системе «Интернет-банк» будет завершена и отобразится форма ввода 5-значного Пин-кода, который в дальнейшем будет использован для быстрого и удобного входа в Мобильное приложение. Если устройство поддерживает функционал сканирования отпечатка пальца Touch ID и/или Face ID, то будет предложена возможность входа в Мобильное приложение по ним.

Вход по отпечатку пальца



Прикоснитесь к сенсору

ОТМЕНА

7. Вход в Систему

Обратите внимание! Если вы регистрировались в офисе Банка или с помощью терминала самообслуживания, то при первом входе в Систему в поле Логин необходимо ввести значение, которое было выдано вам на бумажном носителе или в SMS-сообщении, в поле Пароль – Транспортный пароль, который был отправлен в SMS-сообщении, а затем нажать кнопку **«Войти»**. Далее необходимо произвести смену Транспортного Логина и Пароля на постоянный. Действия по смене Логина и Пароля описаны в пункте 8 **«Изменение логина и пароля»**.

Обратите внимание! При неправильном вводе пароля три раза подряд Клиент автоматически блокируется Системой на 30 минут. Вы можете войти в Систему через полчаса либо получить новый пароль. (Подробнее см. п. 9 **«Забыли логин или пароль»**).

Обратите внимание! Если вход в Систему осуществляется с нового устройства Клиента или используется другой состав программного обеспечения такого устройства, то для такого входа могут быть запрошены дополнительные данные, в частности Разовый код безопасности. После ввода кода из соответствующего SMS-сообщения устройство Клиента будет добавлено в список доверенных устройств этого Клиента и при последующих входах этого Клиента с этого устройства и программного обеспечения подобное подтверждение дополнительным кодом не потребуется.

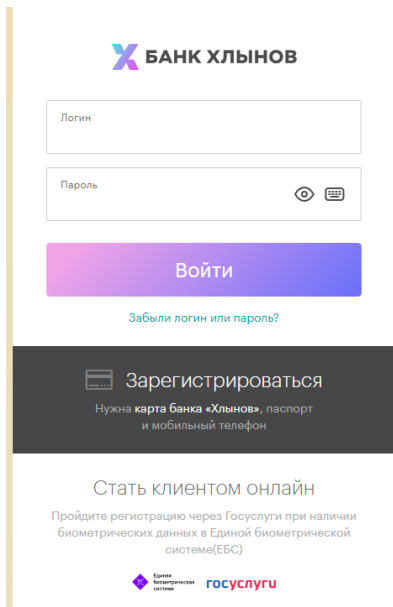
а. На Официальном сайте Банка

Зайдите на Официальный сайт Банка (<https://www.bank-hlynov.ru/>), в верхней правой части страницы из выпадающего меню **«Интернет-банк»** выберите раздел **«Частным клиентам»**

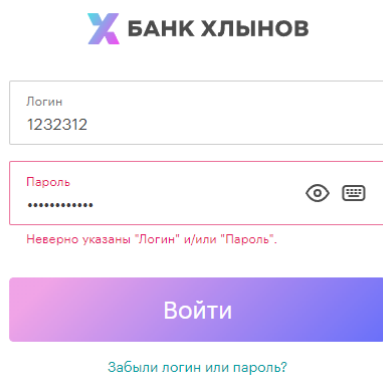


В результате откроется страница входа в Систему. На эту страницу также можно попасть, введя в адресной строке браузера адрес <https://my.bank-hlynov.ru/>. Если вы регулярно пользуетесь Системой «Интернет-банк», рекомендуем добавить этот адрес в закладки.

Для входа в Систему введите Логин и Пароль в соответствующие поля, а затем нажмите кнопку **«Войти»**.

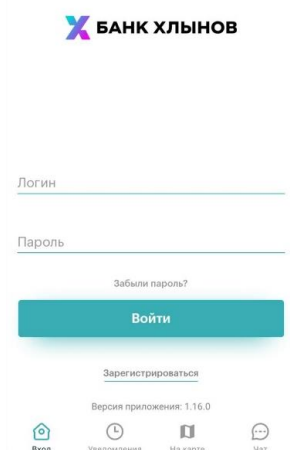


Если поле Логин или Пароль заполнены неверно, появится соответствующая всплывающая подсказка.



в. С использованием Мобильного приложения

Для входа в Систему введите Логин и Пароль в соответствующие поля, а затем нажмите кнопку «Войти».



Отобразится форма ввода 5-значного Пин-кода, который в дальнейшем будет использован для входа в Мобильное приложение. При создании ПИН-кода нельзя использовать простые сочетания цифр (12345, 11111, 55555, 54321 и т.д.). Если Мобильное устройство поддерживает функционал сканирования отпечатка пальца Touch ID и/или Face ID, то будет предложена возможность входа в Мобильное приложение по ним.

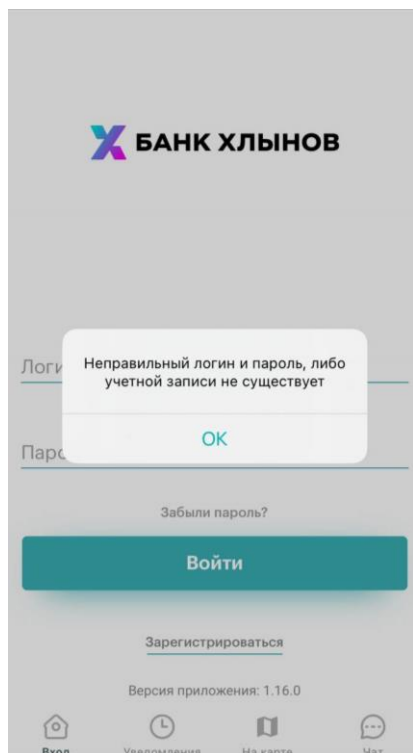
Вход по отпечатку пальца



Прикоснитесь к сенсору

ОТМЕНА

Если поле Логин или Пароль заполнены неверно, появится соответствующая всплывающая подсказка.



8. Изменение Логина и Пароля

Если вы регистрировались в офисе Банка или с помощью терминала самообслуживания, то при первом входе в Систему в поле Логин необходимо ввести значение, которое было выдано вам на бумажном носителе или в SMS-сообщении, в поле Пароль – Транспортный пароль, который был отправлен в SMS-сообщении, а затем нажать кнопку «Войти». Далее необходимо произвести смену Транспортного Логина и Пароля на постоянный.

Для смены Транспортного пароля при первом входе в Систему будет открыто соответствующее окно:

Смена пароля

Пароль должен отвечать следующим требованиям:

- длина от 8 до 30 символов;
- состоит из букв латинского алфавита в разных регистрах и как минимум одной цифры;
- не должен содержать 3 и более одинаковых символов или цифр подряд;
- может содержать элементы пунктуации из списка: «!», «@», «#», «\$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «=», «:», «;», «», «.».

ВЫХОД

ПРОДОЛЖИТЬ

На данной странице необходимо задать постоянный пароль и нажать кнопку «Продолжить». Для подтверждения смены Пароля вам будет отправлено SMS-сообщение с Разовым кодом безопасности, который необходимо ввести в соответствующее поле:

Подтверждение установки нового пароля

Отправлено сообщение, содержащее код подтверждения операции.
Не пришла СМС? [Отправить ещё раз.](#)

При успешном подтверждении WEB-версии Системы «Интернет-банк» откроется страница «**Настройки профиля**», в которой можно будет изменить Логин. В целях безопасной работы с Системой «Интернет-банк» и защиты финансовых операций настоятельно рекомендуется произвести изменение Логина при первом входе в Систему. Для этого необходимо задать новый Логин и нажать кнопку «**Сохранить**»:

Личные данные **Настройки профиля** Мои заявления Безопасность

Настройки профиля

Логин

Логин — это имя для входа в интернет-банк, которое Вы придумали во время регистрации. После смены логина, в форме для входа в интернет-банка будет действовать только новый логин. Логин должен отвечать следующим требованиям: длина от 6 до 30 символов, состоит из букв латинского алфавита, цифр 0-9. Не рекомендуем в качестве логина указывать номер телефона или e-mail. После смены логина рекомендуем осуществить выход и повторить вход в интернет-банк.

Пароль

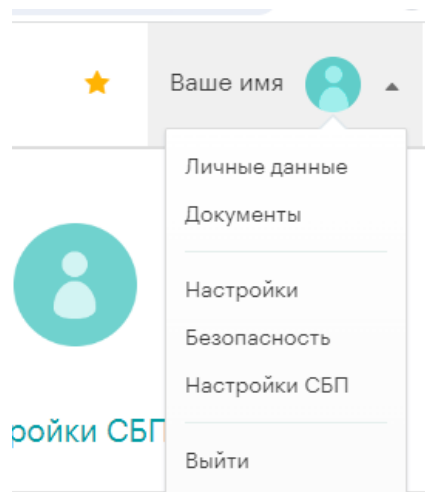
Пароль должен отвечать следующим требованиям: длина от 8 до 30 символов, состоит из букв латинского алфавита в разных регистрах и как минимум одной цифры. Пароль не должен содержать 3 и более одинаковых символов подряд, может содержать элементы пунктуации из списка: «!», «@», «\$», «%», «^», «&», «*», «(», «)», «_», «=», «>», «<», «:», «;», «,», «.». Не рекомендуем в качестве пароля указывать номер телефона или e-mail. После смены пароля рекомендуем осуществить выход и повторить вход в интернет-банк.

**Блокировка
учётной записи**

Функция временно блокирует доступ в Интернет-банк. Для восстановления доступа потребуется паспорт и номер банковской карты. Внимание! После подтверждения произойдет мгновенная блокировка и выход из системы.
Внимание! После подтверждения произойдет блокировка и выход из системы.

В дальнейшем для входа в Систему необходимо будет использовать Постоянные Логин и Пароль.

Смену Логина и Пароля можно осуществить в любой момент пользования Системой. Для этого необходимо перейти в WEB-версию Системы «Интернет-банк» и нажать кнопку «**Настройки**» в выпадающем меню в правом верхнем углу страницы.



9. Забыли логин или пароль

Обратите внимание! При составлении Логина и Пароля рекомендуем вам пользоваться правилами, описанными в разделе 6 «**Требования безопасности для логина и пароля**». В случае если вы забыли Пароль или Логин, воспользуйтесь функцией «**Забыли логин или пароль?**».

A login form for X-BANK ХЛЫНОВ. The form features the bank's logo at the top, followed by two input fields: "Логин" and "Пароль". The "Пароль" field includes an eye icon for toggling visibility and a keyboard icon. Below the input fields is a large, gradient-colored button labeled "Войти". At the bottom of the form, there is a red-bordered button labeled "Забыли логин или пароль?".

После нажатия кнопки «**Забыли логин или пароль?**» система предложит ввести данные Банковской карты и документа, удостоверяющего личность. Для восстановления доступа к Системе необходимо ознакомиться с Условиями обслуживания в интернет-банке АО КБ «Хлынов» и отметить пункт «Ознакомлен и согласен с Условиями обслуживания в интернет-банк АО КБ «Хлынов».

Проверка карты

Номер карты

Номер карты расположен на её лицевой стороне.

Серия
паспорта

Номер паспорта

Ознакомлен и согласен с
условиями обслуживания в
интернет-банке АО КБ
«Хлынов»

ПРОДОЛЖИТЬ

После нажатия кнопки «**Продолжить**» необходимо ввести Разовый код безопасности из SMS-сообщения.

СМС-подтверждение

СМС-код

Сейчас Вы получите СМС с кодом идентификации

Не пришла SMS? [Повторить](#)

ПРОДОЛЖИТЬ

В появившемся окне «**Создание профиля**» нужно указать желаемые Логин и Пароль (необходимо повторить Пароль в поле «Повторить пароль»).

Создание профиля

Логин

Пароль

Повторите пароль

Логин должен отвечать следующим требованиям:

- длина от 6 до 30 символов;
- состоит из букв латинского алфавита, цифр 0-9 и специальных символов «@», «_», «-»;
- регистр букв значение не имеет.

Пароль должен отвечать следующим требованиям:

- длина от 8 до 30 символов;
- состоит из букв латинского алфавита в разных регистрах и как минимум одной цифры;
- не должен содержать 3 и более одинаковых символов или цифр подряд;
- может содержать элементы пунктуации из списка: «!», «@», «#», «\$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «=», «:», «;», «», «.».

СОХРА!

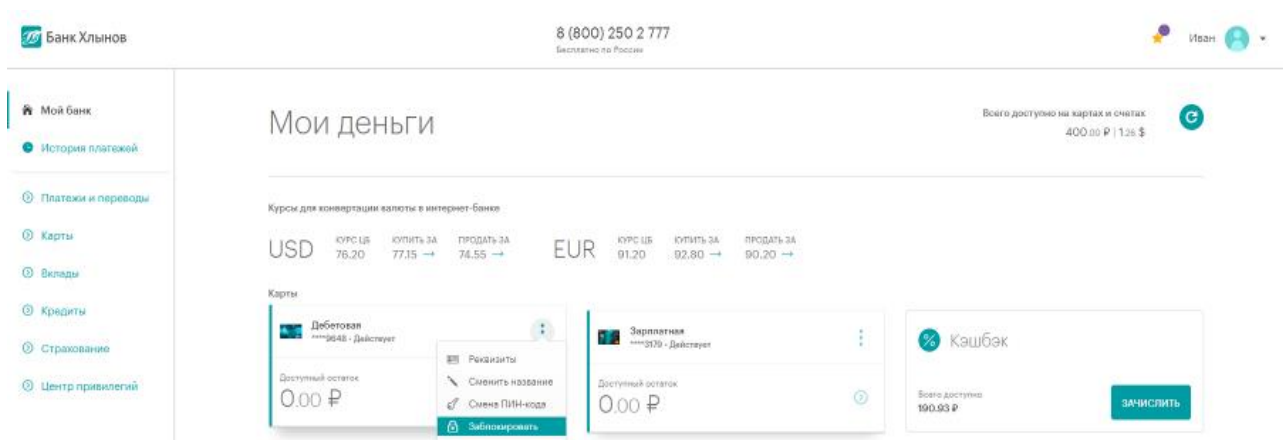
10. Блокировка Карты

В случае утери Карты, а также если у вас есть основания полагать, что данные Карты были скомпрометированы или по ней пытаются провести мошенническую операцию, в целях безопасности необходимо произвести Блокировку Карты.

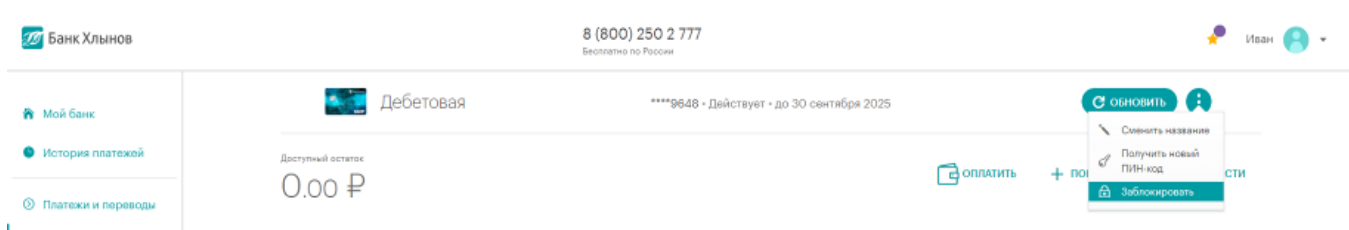
Разблокировка производится в офисе Банка при личном присутствии владельца Карты, наличии оригинала документа, удостоверяющего личность, и письменного заявления на разблокировку Карты или при обращении в Чат после входа в Систему.

1) В Web-версии Системы «Интернет-банк»

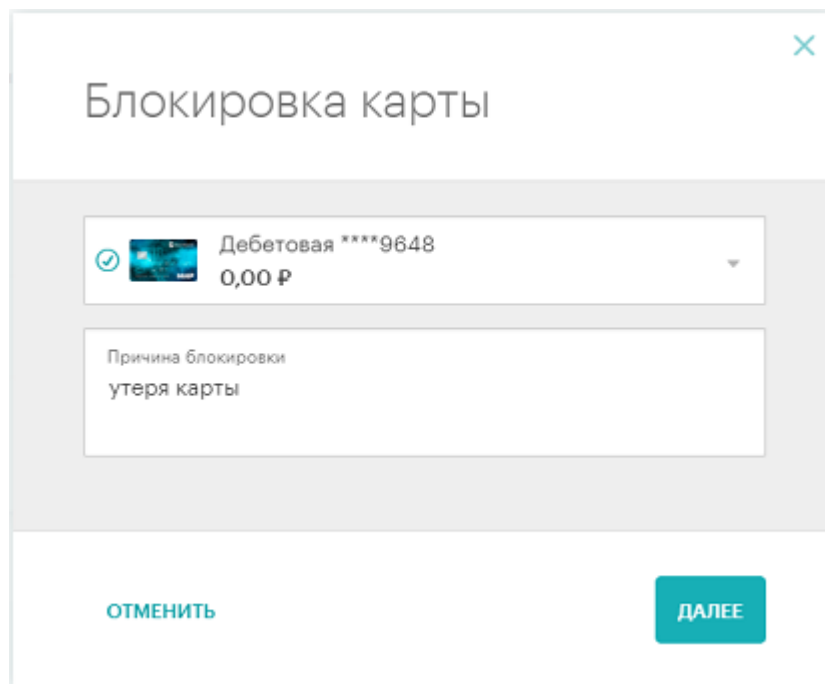
Заблокировать Карту вы можете находясь на главной странице Системы с помощью кнопки «Заблокировать» в выпадающем меню:



Также возможность заблокировать Карту предоставлена на странице детальной информации по Карте из выпадающего меню:



В результате откроется окно блокировки Карты, в котором необходимо указать причину блокировки. В случае выбора не той Карты, ее можно изменить из выпадающего списка Карт.



Блокировка карты

Дебетовая ****9648
0,00 Р

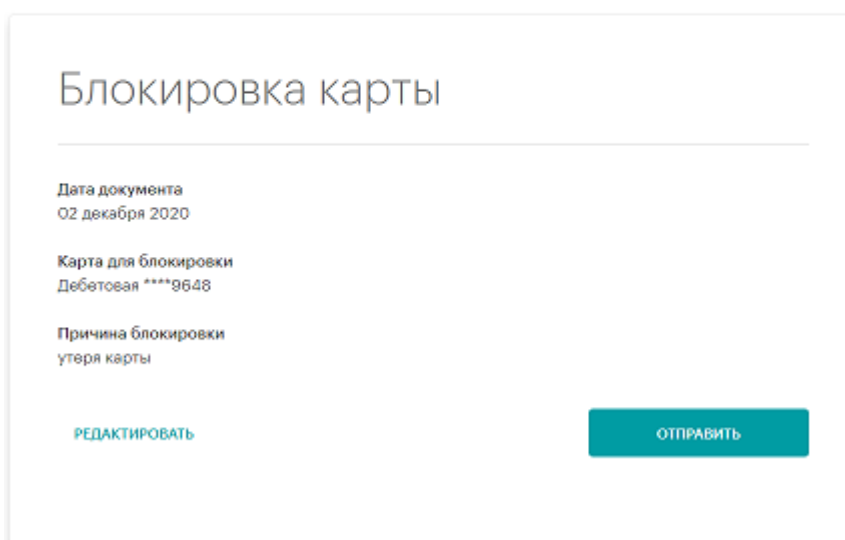
Причина блокировки
утеря карты

ОТМЕНИТЬ ДАЛЕЕ

После того как все необходимые сведения внесены, нажмите кнопку «**Далее**». Система выведет на экран форму подтверждения заявления на блокировку Карты, на которой вам необходимо проверить введенные данные и нажать кнопку «**Отправить**».

Шаг 2/2

Подтверждение заявления



Блокировка карты

Дата документа
02 декабря 2020

Карта для блокировки
Дебетовая ****9648

Причина блокировки
утеря карты

РЕДАКТИРОВАТЬ ОТПРАВИТЬ

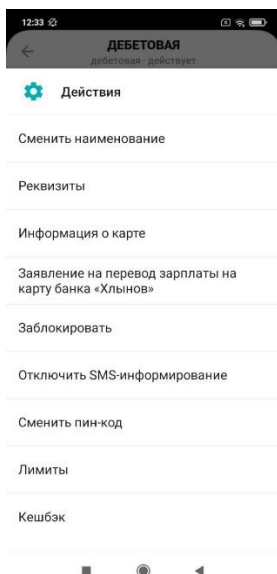
Если Вы передумали отправлять заявку на блокировку Карты, то нажмите кнопку «**Редактировать**», затем – «**Отменить**».

После проверки всех данных по кнопке «**Отправить**» откроется заполненная форма заявления, в которой нужно подтвердить операцию Разовым кодом безопасности.

2) С использованием Мобильного приложения

Возможность заблокировать Карту представлена на странице детальной информации по Карте с

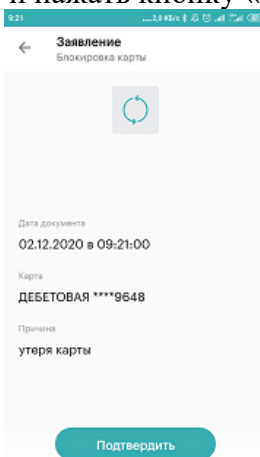
помощью кнопки «Действия» с иконкой шестеренки. В выпадающем меню необходимо выбрать «Заблокировать»:



В результате откроется окно блокировки Карты, в котором необходимо указать причину блокировки, ознакомиться с информацией Банка и нажать кнопку «Далее».



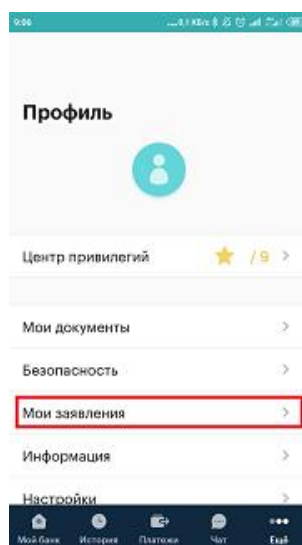
Система выведет на экран форму подтверждения заявления на блокировку Карты, на которой вам необходимо проверить введенные данные и нажать кнопку «Подтвердить».



После подтверждения откроется экран для ввода Разового кода безопасности из SMS-сообщения,

такой код необходим для завершения операции.

Статус заявления на блокировку Карты можно посмотреть в разделе: «Еще» → «Мои заявления».

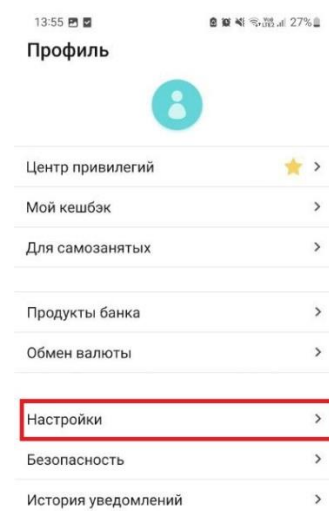
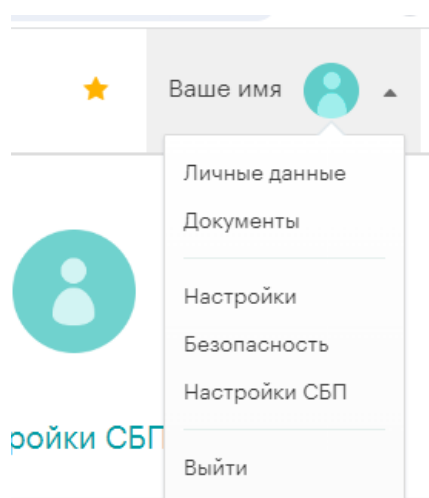


11. Личные данные

Чтобы перейти в раздел с личными данными, необходимо в правом верхнем углу нажать на ваше имя и в выпадающем меню выбрать пункт «Личные данные»

В разделе «Личные данные» Web-версии Системы «Интернет-банк» могут отображаться номер телефона, на который поступают SMS-сообщения, адрес электронной почты, а также информация о добавленных документах для поиска начислений в государственных информационных системах (ГИС ГМП и ГИС ЖКХ), отдельный элемент интерфейса «Актуализировать» предоставляет возможность актуализировать паспортные данные, в случае необходимости.

Электронный почтовый адрес необходим для направления Клиенту Банком писем информационного характера, а также связи в случае необходимости. Чтобы добавить электронную почту необходимо нажать «Добавить», ввести в открывшемся окне свой адрес электронной почты и нажать на кнопку «Сохранить».



Разделы «Мои документы» (на сайте) и «Для поиска начислений» (в мобильном приложении) предоставляют возможность управлять перечнем документов для оперативного поиска информации о

начислениях по налогам, штрафам, пени и другим платежам в пользу государственных служб. Поиск начислений происходит по документам, добавленным Клиентом в Систему, а также по документам и идентификаторам объектов (движимое и недвижимое имущество, единым лицевым счетам квартир и т.д.), которыми располагает Банк. В частности, отображение информации о начисленных штрафах ГИБДД осуществляется по номеру водительского удостоверения и номеру свидетельства о регистрации транспортного средства, задолженность по налогам – по ИНН.

Для добавления документа необходимо нажать «Добавить новый документ», выбрать тип документа, ввести его номер и нажать на кнопку «Сохранить».

Личные данные Настройки профиля Мои заявления Безопасность Настройки СБП

Телефон и e-mail

Мобильный телефон +7 (900) 000-00-00
Номер телефона, на который мы отправляем СМС-оповещения и СМС-коды для подтверждения операций в интернет-банке.

E-mail e-mail@domen.ru
Электронный почтовый адрес, на который мы можем отправить Вам информацию о новых функциях, персональных предложениях, тарифах, и связаться с Вами в случае необходимости.

Паспортные данные Актуальные
Если у Вас изменились паспортные данные — приложите фото или скан-копии документов.

Мои документы
Для автоматического поиска налогов, штрафов ГИБДД, счетов и оплаты начислений в системах ГИС ГМП, ГИС ЖЖХ укажите данные паспорта, водительского удостоверения или любого другого документа. Система ежедневно ищет свежие начисления и напоминает вам об оплате.

+
ДОБАВИТЬ НОВЫЙ ДОКУМЕНТ

15:24 VoLTE 4G 33%

← **Документы для поиска начислений** ⋮

Документы нужны, чтобы искать и оплачивать в интернет-банке начисления и счета по налогам, штрафам ГИБДД, в пенсионном фонде. А также в других организациях через государственные системы ГИС ГМП и ГИС ЖЖХ.

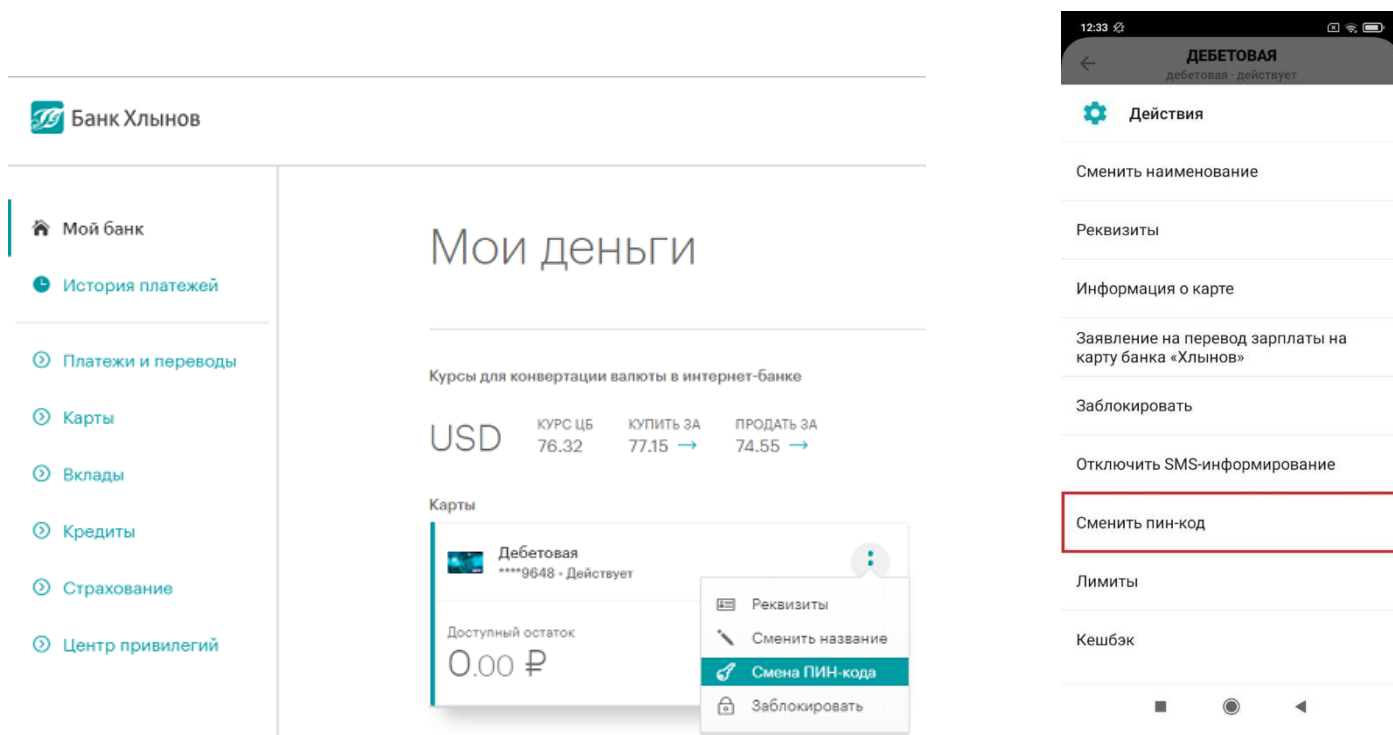
Добавить новый документ +


12. Смена ПИН-кода Карты

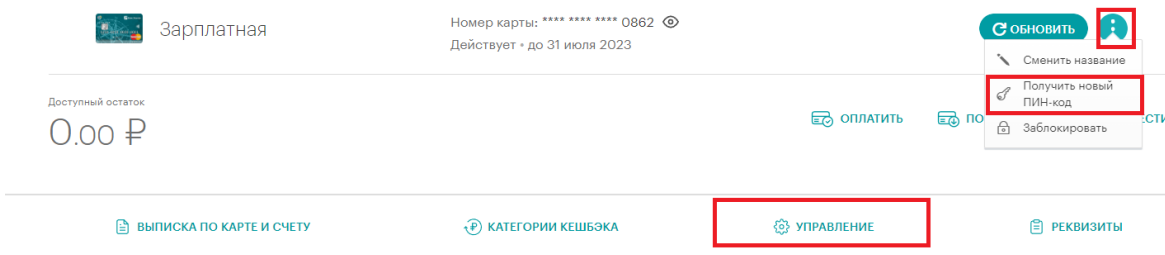
Обратите внимание! В целях безопасности: не сообщайте ПИН-код Карты третьим лицам. Помните, что сотрудники Банка никогда не попросят вас назвать ПИН-код.

Функция смены ПИН-кода может потребоваться в ситуации, когда вы забыли ПИН-код своей Карты или подозреваете, что он стал известен посторонним людям. В целом, рекомендуется периодически менять ПИН-код для предотвращения несанкционированного использования Карты.

Сменить ПИН-код возможно с главной страницы Системы с помощью кнопки «Смена ПИН-кода» в выпадающем меню Карты (в WEB-версии Системы «Интернет-банк») или через кнопку «Действия» в Карте (через мобильное приложение):



Также в WEB-версии смена ПИН-кода возможна со страницы детальной информации по карте из выпадающего меню  или во вкладке «Управление» с помощью кнопки «СМЕНИТЬ ПИН-КОД»:



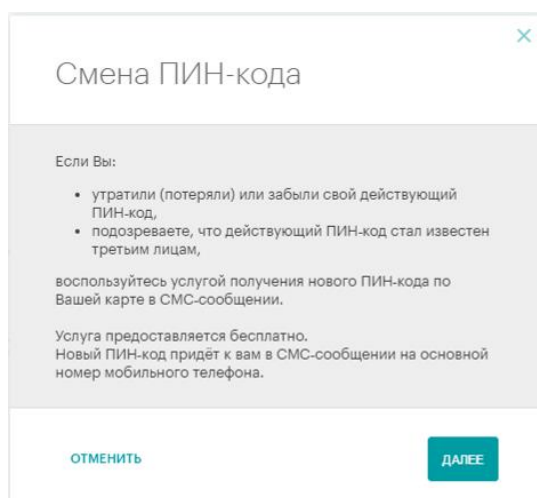
Управление картой

Смена ПИН-кода

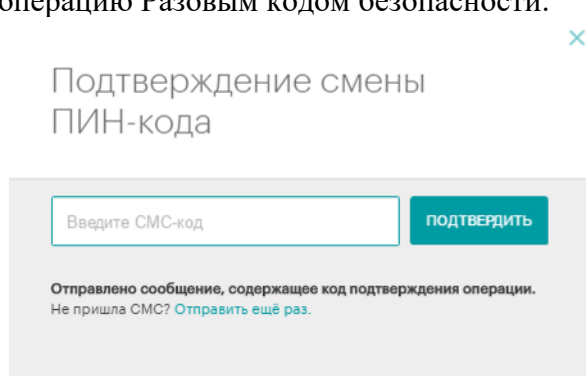
Получите новый ПИН-код, если потеряли, забыли или подозреваете, что Ваш действующий ПИН-код стал известен третьим лицам. Новый ПИН-код придёт в СМС-сообщении. Услуга предоставляется бесплатно.

СМЕНИТЬ ПИН-КОД

В результате откроется окно смены ПИН-кода Карты, в котором указана информация об условиях совершения операции. Если вы передумали отправлять заявку на смену ПИН-кода, то нажмите кнопку «Отменить».



После нажатия кнопки «Далее» Система выведет на экран форму подтверждения смены ПИН-кода, в которой нужно подтвердить операцию Разовым кодом безопасности.



Основные правила обеспечения безопасности ваших средств на Карте:

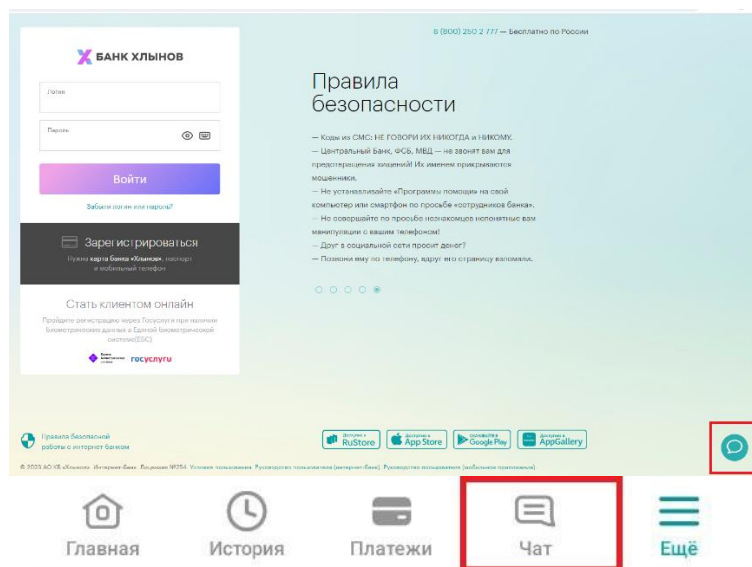
- не записывайте ПИН-код на Карте и не храните их вместе;
- не передавайте Карту и сведения о ПИН-коде третьим лицам. Право пользования Картой принадлежит только ее держателю;
- не сообщайте данные вашей Карты (номер Карты, срок действия, CVC) и ПИН-код по

- телефону или электронной почте;
- не вводите ПИН-код при расчетах через сеть Интернет.

13. Чат

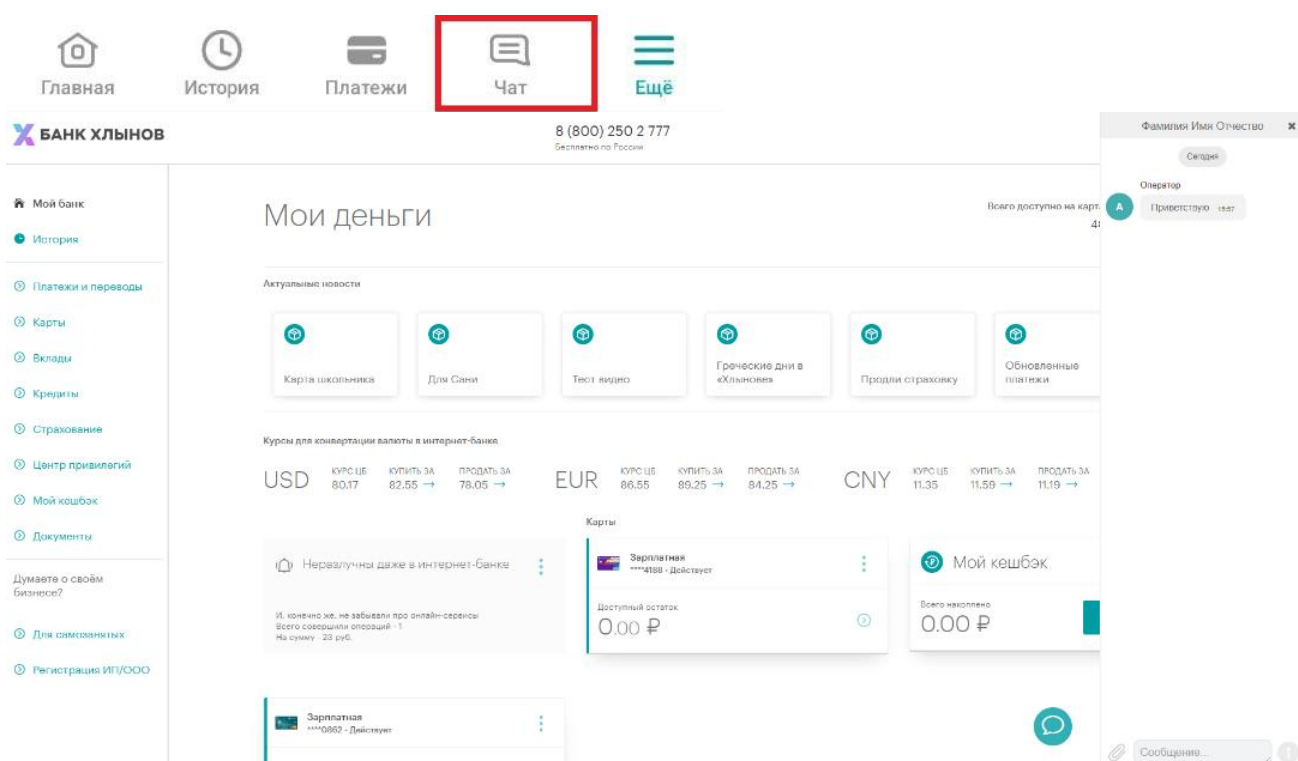
Чат – это сервис для предоставления консультаций пользователям Системы «Интернет-банк» в режиме реального времени.

Для получения консультации достаточно перейти в раздел Чата в нижнем правом углу страницы входа в Систему и задать интересующий вопрос.



Клиент, авторизованный в Системе (совершил вход в Систему с использованием Логина и Пароля или короткого Пин-кода при использовании Мобильного приложения), имеет возможность вести персонализированную электронную переписку с Банком. В этом случае Банк может направлять на исполнение заявления от Клиента о совершении операций, обмениваться информацией с Клиентом в

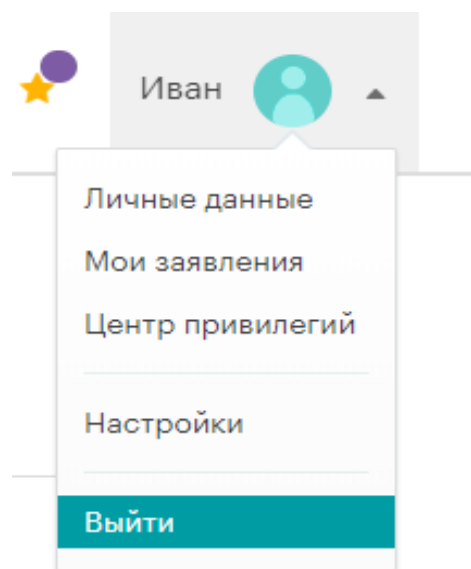
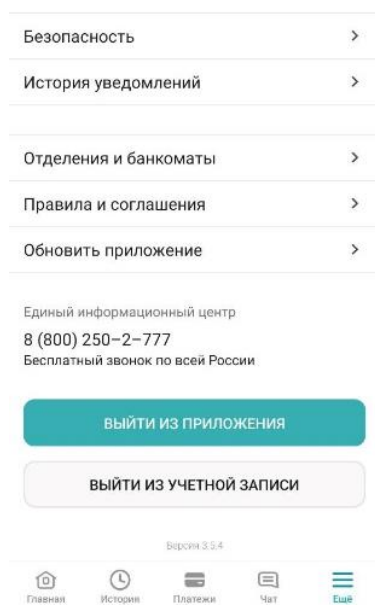
соответствии с действующим законодательством. Данная переписка является юридически значимой, как если бы она осуществлялась на бумажных носителях с подписью уполномоченных лиц¹.



¹ Часть 2 статьи 5 и часть 2 статьи 6 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

14. Выход из Системы

Для безопасного выхода из Системы нажмите кнопку **«Выйти»**, расположенную в выпадающем меню в правом верхнем углу страницы (в WEB-версии Системы «Интернет-банк»), или кнопку **«Выйти из приложения»**, расположенную в **«Еще»**.



Обратите внимание! В случае если вы не совершаете активных действий в Системе, рабочая сессия продолжает оставаться активной в течение 12 минут, после чего произойдет автоматический выход. Для дальнейшей работы вам необходимо снова **войти в Систему**.

15. Требования безопасности

Технологии защиты операций в Системе используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень ее надежности и безопасности. Вместе с тем эффективность данных механизмов зависит также и от соблюдения вами определенных мер безопасности.

В целях безопасной работы с Системой и защиты ваших финансовых операций просим внимательно ознакомиться с Правилами безопасности.

1) Безопасность при использовании сайта

– **«Страница входа»** в Систему содержит **только поля для ввода Логина и Пароля**. В случае если на данной странице вас просят ввести любую другую персональную информацию (номера Банковских карт, Номер мобильного телефона, другие личные данные), не выполняйте никаких операций и обратитесь в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный);

– нельзя сообщать свои конфиденциальные данные третьим лицам, в том числе родителям, близким родственникам и сотрудникам Банка. К таким данным относятся реквизиты Карты, ПИН-код, Пароль и Логин от Системы, а также Разовые коды безопасности для совершения операций;

– Система **никогда не отправляет Клиентам коды для отмены операций**. Если вам

предлагается ввести код для отмены операции, то необходимо выйти из Системы и сразу же обратиться в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный);

– **при утрате мобильного телефона** или иного устройства, с которых ранее осуществлялся вход в Систему, следует незамедлительно обратиться к своему оператору сотовой связи для **блокировки SIM-карты** и в Единый сервисный центр Банка для блокировки Системы или внесения изменений в список доверенных устройств;

– **не устанавливайте на телефон**, на который приходят SMS-сообщения из Банка, **приложения, полученные из ненадежных источников**. Помните, что Банк **не рассылает** своим клиентам ссылки или указания по установке приложений через **SMS/MMC/Email-сообщения**;

– в начале работы с Системой убедитесь в том, что **защищенное соединение установлено именно с официальным сайтом** услуги (<https://my.bank-hlynov.ru>); (Подробнее см. п. 17 «Проверка подлинности сайта»);

– используйте **современные антивирусные программы**, следите за их **обновлением** и регулярно выполняйте **антивирусную проверку** на своих устройствах;

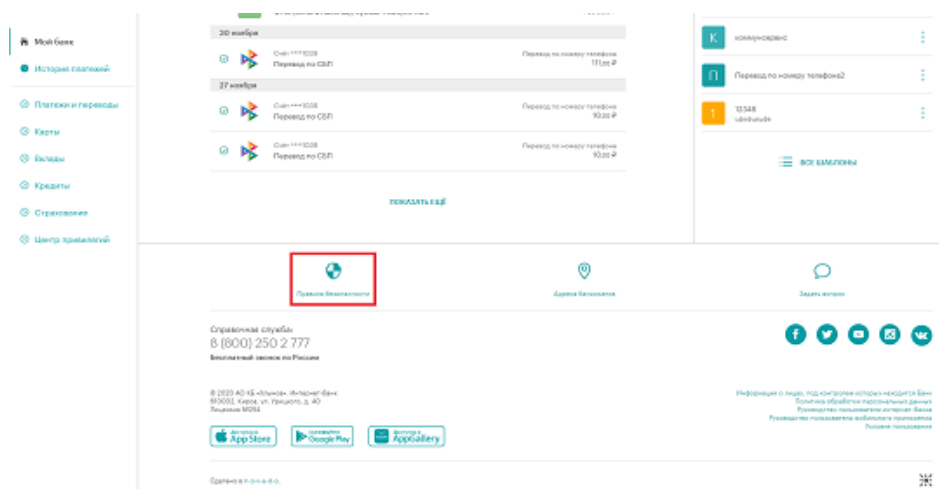
– **своевременно устанавливайте обновления** программного обеспечения своих устройств, рекомендуемые компанией-производителем;

– рекомендуем использовать **дополнительное программное обеспечение**, позволяющее повысить уровень защиты ваших устройств, например, программы поиска шпионских компонент, программы защиты от спам-рассылок и пр.;

– для безопасного завершения работы с Системой необходимо нажимать на кнопку **«Выйти»**, но не просто закрывать окно браузера;

– после работы с публичного устройства (интернет кафе, устройств, которые вам не принадлежат) рекомендуем выполнить процедуру смены Пароля;

Вы всегда можете ознакомиться с Правилами безопасности системы «Интернет-банк» по ссылке, расположенной внизу страницы:



Если у вас есть подозрения, что кто-либо использует ваш Логин и Пароль или, совершаются операции, которых вы не совершали, необходимо обратиться в Банк. Помните, что при работе со

своими счетами в Системе следует быть такими же внимательными и бдительными, как при обращении с наличными средствами в вашем кошельке.

2) Безопасность при использовании Мобильного приложения

– экран для входа в Мобильное приложение содержит **только поля для ввода Логина и Пароля**. В случае если на данном экране появляются поля, в которые вас просят ввести любую другую персональную информацию (номера Карт, Номер мобильного телефона, другие личные данные), не выполняйте никаких операций через Мобильное приложение и обратитесь в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный);

– нельзя сообщать свои конфиденциальные данные третьим лицам, в том числе родителям, близким родственникам и сотрудникам Банка. К таким данным относятся реквизиты Карты, ПИН-код, Пароль и Логин от Системы, а также Разовые коды безопасности для совершения операций;

– всегда проверяйте номер телефона, с которого приходят SMS-уведомления от Банка. АО КБ «Хлынов» всегда отправляет сообщения от абонента: bank-hlynov;

– Клиент должен использовать только Мобильные приложения, распространяемое Банком, для входа в Систему, доступные в официальных магазинах: Google Play Market, Apple Store, Huawei AppGallery, RuStore. Обязательно убедитесь, что в поле «разработчик мобильного приложения» указан АО КБ «Хлынов»;

– при создании короткого ПИН-кода для быстрого входа в Мобильное приложение нельзя использовать простые сочетания цифр (12345, 11111, 55555, 54321 и т.д.);

– на мобильное устройство, которое используется для входа в Систему, необходимо установить современный антивирус, который защитит устройство от действия вредоносных программ;

– Система **никогда не отправляет клиентам коды для отмены операций**. Если вам предлагается ввести код для отмены операции, то необходимо выйти из Системы и сразу же обратиться в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный);

– **не устанавливайте на телефон**, на который приходят SMS-сообщения из Банка, **приложения, полученные из ненадежных источников**. Помните, что Банк **не рассылает** своим Клиентам ссылки или указания по установке приложений через **SMS/MMC/Email-сообщения**;

– для безопасного завершения работы с Системой необходимо нажимать на кнопку **«Выйти из приложения»**, а не сворачивать Мобильное приложение;

– рекомендуется установить в телефоне/смартфоне и ином Мобильном устройстве пароль для доступа к устройству, данная возможность доступна для большинства современных моделей устройств;

– **при утере мобильного телефона** или иного Мобильного устройства, с которого ранее осуществлялся доступ к Системе, следует незамедлительно обратиться к своему оператору сотовой связи для **блокировки SIM-карты** и в Единый сервисный центр банка по телефону 8 (800) 250-2-777 (звонок по России бесплатный);

– при смене Номера мобильного телефона, на который подключена услуга «SMS-информирование» необходимо обратиться в любое подразделение Банка и оформить заявление на

смену Номера мобильного телефона;

– будьте внимательны – не оставляйте свои Мобильные устройства без присмотра, чтобы исключить несанкционированное использование Мобильного приложения и внесения изменений в настройки устройств;

– своевременно устанавливайте доступные обновления операционной системы и приложений на ваши Мобильные устройства/телефон;

– на смартфонах и иных Мобильных устройствах, с которых ранее осуществлялся доступ к Системе, необходимо использовать антивирусные программы, доступные в магазинах мобильных приложений, в том числе бесплатно;

– перед началом работы в Системе убедитесь в правильности установленного на Мобильном устройстве времени. В случае существенного отличия времени, установленного на телефоне от текущего времени часового пояса вашего местонахождения, вход и работа в Системе, совершение операций в ней могут быть ограничены;

– не устанавливайте на свои Мобильные устройства/телефон нелицензионные операционные системы, так как это отключает защитные механизмы, заложенные производителем мобильной платформы, и они могут быть уязвимым к действия вредоносного программного обеспечения;

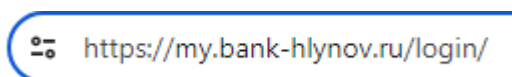
Если у вас есть подозрения что кто-либо использует ваш Логин и Пароль или совершаются операции, которых вы не совершали, необходимо обратиться в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный). Помните, что при работе со своими счетами в Системе «Интернет-банк» следует быть такими же внимательными и бдительными, как при обращении с наличными денежными средствами в вашем кошельке.

16. Проверка подлинности сайта

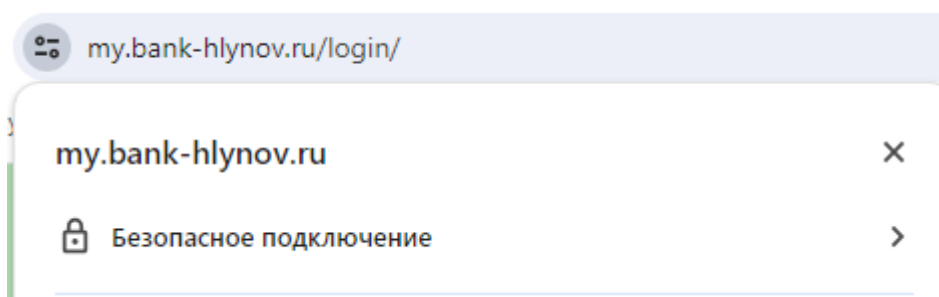
Для надежной работы в Системе рекомендуется использовать современные Интернет-браузеры, например, Chrome, Яндекс браузер.

В целях дополнительной защиты при входе в систему «Интернет-банк» рекомендуем проверять подлинность сайта до ввода Логина и Пароля. Для этого выполните следующие действия:

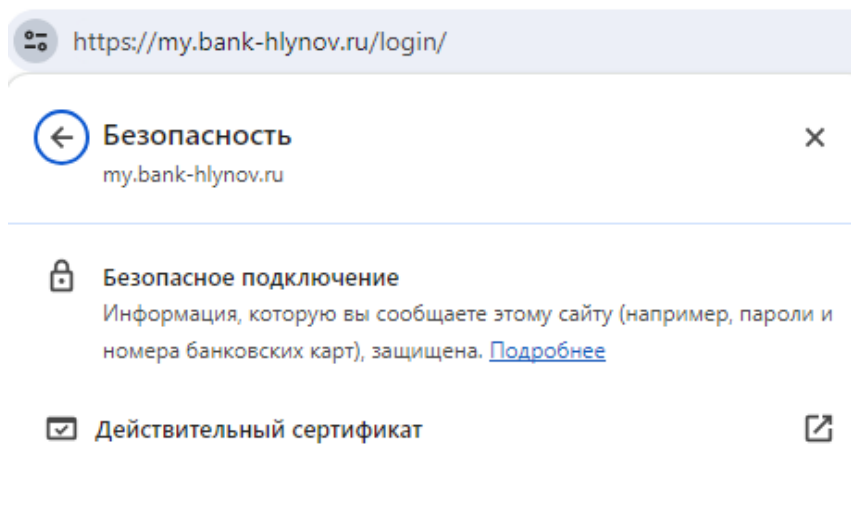
1. Проверьте адрес в адресной строке браузера: <https://my.bank-hlynov.ru/>



2. Нажмите на значок «Сведения о сайте» слева от адресной строки:

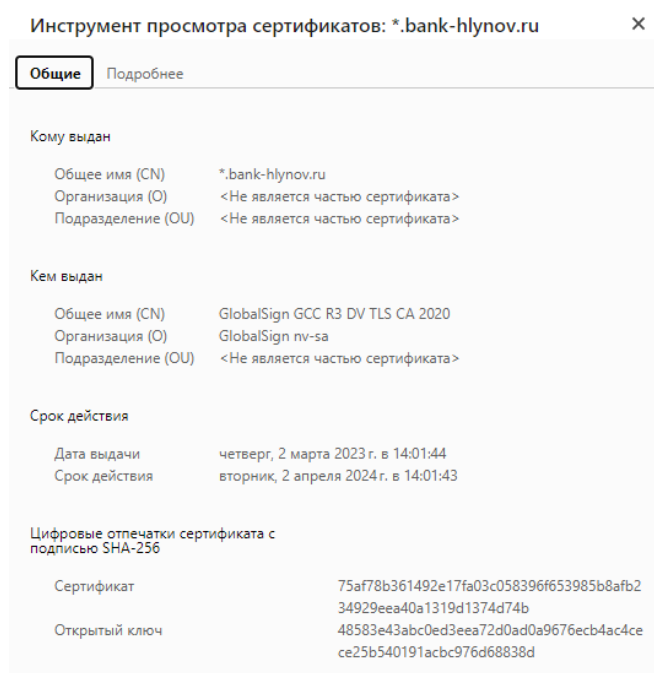


3. В открывшемся списке выберите пункт «**Безопасное подключение**», затем «**Действительный сертификат**»:



Откроется новое окно со всеми данными о SSL сертификате.

4. В открывшемся окне вы можете увидеть следующую информацию:



Кому выдан - поле указывает домен, для которого выдан SSL сертификат. Если он не совпадает с доменом, на который вы планировали попасть, возможно, сайт подменен.

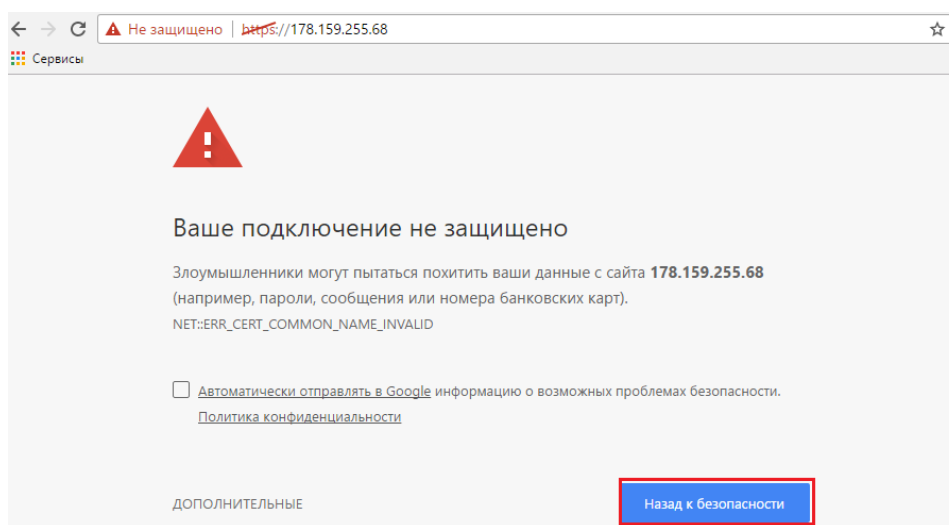
Кем выдан показывается название центра сертификации, ответственного за выдачу сертификата. К наиболее доверенным ЦС относятся Comodo, Symantec, Thawte, GeoTrust, GlobalSign, AlphaSSL и RapidSSL, и некоммерческий Let's Encrypt. Желательно не доверять сайтам с сертификатами от малоизвестных сертификационных центров, так как они могут более легко выдать сертификаты неправомерным получателям.

Срок действия показывает период действия SSL сертификата.

Далее можно закрыть окно с информацией о сертификате.

Обратите внимание! При появлении окна «Предупреждение Системы безопасности», указывающего на проблемы проверки сертификата сайта, вводить идентификаторы пользователя **нельзя**. Вводимые данные могут стать доступны третьим лицам.

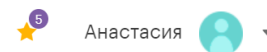
Пример предупреждения системы безопасности:



После входа в Систему убедитесь, что отображенные на стартовой странице имя и фамилия соответствуют вашим.



8 (800) 250 2 777
Бесплатно по России



Обратите внимание! При любых подозрениях на выполнение несанкционированных вами операций следует незамедлительно обратиться в Единый Сервисный Центр Банка для принятия решения о блокировке Банковской карты и/или доступа к Системе по телефону **8 (800) 250-2-777 (звонок по России бесплатный)**.