УСЛОВИЯ
предоставления услуги «Интернет-банк» физическим лицам

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

1.1. Авторизация – подтверждение полномочий (предоставление прав доступа) Клиента, успешно прошедшего Идентификацию и Аутентификацию, на получение услуг Банка, предусмотренных настоящими «Условиями предоставления услуги «Интернет-банк» физическим лицам» (далее – Условия), с использованием Системы «Интернет-банк» (далее-Система) на протяжении одного Сеанса связи.

1.2. АС Фид-Антифрод - автоматизированная система ФинЦЕРТ Банка России, предназначенная для выполнения норм Федерального закона от 27.06.2018 № 167-ФЗ в части создания, формирования и ведения базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры данных из этой базы.

1.3. Аутентификация – процесс проверки подлинности пользователя в Системе при обращении в Банк для совершения банковских операций и/или получения информации по Счетам дистанционно и совершения иных действий в порядке, предусмотренном настоящими Условиями.

1.4. Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора пользователя Системы. Может состоять, не ограничиваясь, из Номера мобильного телефона, уникальных Логина и Пароля. Необходима для доступа к Системе «Интернет-банк» и оказания услуг дистанционного банковского обслуживания Банком.

1.5. Банк – коммерческий банк «Хлынов» (акционерное общество).

1.6. Банковский счет (Счет) – банковский счёт Клиента, открытый в Банке в рамках соответствующего договора для совершения Клиентом расчетных и кассовых операций, не связанных с осуществлением предпринимательской деятельности.

1.7. Доверенное устройство – мобильное устройство, зарегистрированное в Системе, для входа с которого не требуется проходить дополнительную проверку безопасности.

1.8. Договор – договор о предоставлении услуги «Интернет-банк», заключаемый между Банком и Клиентом.

1.9. Доступный остаток – сумма денежных средств, доступных для проведения операций с использованием Системы, включающая остаток собственных средств Клиента на Карточном счете и сумму овердрафта/лимита кредитных средств (при их предоставлении).

1.10. Единый сервисный центр - подразделение Банка, сотрудники которого обрабатывают обращения Клиентов по телефону, электронной почте, веб-форме на официальном сайте Банка, посредством Чата и т.д.

1.11. Заявление на подключение услуги «Интернет-банк» (далее – Заявление) – оферта Клиента о заключении Договора о предоставлении услуги «Интернет-банк», оформленная и направленная в Банк одним из способов, установленных настоящими Условиями.

1.12. Идентификатор пользователя (Логин) – имя пользователя, которое используется для входа в Систему, позволяющее однозначно идентифицировать Клиента в Системе. Может содержать буквы, цифры или символы.

1.13. Идентификация – установление личности Клиента (доверенного лица Клиента) для совершения банковских операций или получения информации по Счетам Клиента и совершении иных действий в порядке, предусмотренном настоящими Условиями.

1.14. Информационный сервис – предоставление Клиенту посредством Системы возможности получения актуальной и достоверной информации о Счетах, дополнительной информации, а также сервисных и других операциях, доступных в Системе.

1.15. Карта – банковская карта международной/национальной платежной системы, предназначенная для совершения операций ее держателем(клиентом).

1.16. Карточный счет (Картсчет) – открытый на имя Клиента банковский счет, используемый для учета операций, совершаемых с использованием Карты/реквизитов Карты, и проведения расчетов в соответствии с договором, не связанных с осуществлением предпринимательской деятельности.

1.17. Клиент (Пользователь Системы) – физическое лицо, заключившее Договор или намеревающееся заключить Договор.

1.18. Компрометация – утрата Банком или Клиентом уверенности в том, что защищаемая информация не может быть использована третьими лицами.

1.19. Мобильная версия Системы «Интернет-банк» (Мобильное приложение) – приложение (программное обеспечение) для мобильных устройств, предоставляющее Клиенту возможность доступа к Системе «Интернет-банк». Перечень Мобильных приложений, порядок их установки на мобильные устройства Клиента и руководство по использованию Мобильных приложений указаны в Руководстве пользователя. Любые электронные документы, передаваемые через Мобильное приложение, а также действия, совершаемые посредством Мобильного приложения, имеют юридическую силу. Банк в любой момент по собственному усмотрению определяет и изменяет перечень банковских операций и функций, доступных в Мобильном приложении, а также устанавливает лимиты на суммы операций в Мобильном приложении.

1.20. Мобильное устройство – смартфоны, планшетные компьютеры и т.п., находящиеся в личном пользовании Клиента, работающие под управлением операционной системы iOS 13 или Android 5.0 и выше.

1.21. Номер мобильного телефона – номер телефона, указанный Клиентом в Заявлении на выпуск карты или открытие счета, хранимый в электронных системах Банка, используемый для связи с Клиентом, для подтверждения операций или Идентификации Клиента. Данные, отправленные на указанный Номер мобильного телефона, считаются безусловно полученными надлежащим пользователем.

1.22. Официальный сайт Банка – сайт Банка в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет), расположенный по адресу https://www.bank-hlynov.ru/.

1.23. Официальный сайт Системы – сайт Интернет-банка в сети Интернет, расположенный по адресу https://my.bank-hlynov.ru.

1.24. Персональный идентификационный номер карты (ПИН-код карты) – число,

являющееся секретным кодом Карты. ПИН-код генерируется с соблюдением конфиденциальности, недоступен сотрудникам Банка, известен только держателю и не подлежит разглашению третьим лицам. Операции по Карте, совершенные с вводом ПИН-кода, приравниваются к операциям, безусловно одобренным и собственноручно подписанным держателем.

1.25. Пин-код для входа в Мобильное приложение – короткая последовательность цифр определяемая и устанавливаема Клиентом после первого входа в Мобильное приложение для более простого и легкого входа в Мобильное приложение без необходимости вводить Логин и Пароль.

1.26. Платежный сервис – предоставление Клиенту посредством Системы возможности совершения операций по распоряжению денежными средствами, в размере Доступного остатка на счетах Клиента, не противоречащих действующему законодательству Российской Федерации и подтвержденных при необходимости с помощью Разового кода безопасности, на основании расчетных документов Клиента.

1.27. Постоянный пароль – секретная последовательность символов, которая известна только Клиенту. Используется для Аутентификации Клиента при входе в Систему.

1.28. Простая электронная подпись (ПЭП) – электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом в соответствии с Договором. ПЭП соответствует признакам и требованиям, предъявляемым к простой электронной подписи Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи" и является аналогом собственноручной подписи Клиента. ПЭП формируется Клиентом посредством прохождения Аутентификации и Авторизации в Системе при помощи Логина, Пароля, Разового кода безопасности, отправляемого Системой в SMS-сообщении и/или при помощи Пин-кода для входа в Мобильное приложение.

1.29. Разовый код безопасности – уникальный набор цифр, отправляемый Клиенту на Номер мобильного телефона, используемый для подтверждения операции/действия.

1.30. Сеанс связи (сессия) – период времени, в течение которого Клиент авторизован для работы в Системе, обеспечивающий непрерывное взаимодействие Банка и Клиента. Для начала Сеанса связи в Системе необходимо успешно пройти Аутентификацию и Авторизацию.

1.31. Сессионный ключ – уникальная последовательность символов, предназначенная для проверки авторства ЭД, направляемых Клиентом в рамках Сеанса связи. Сессионный ключ формируется после успешного прохождения Аутентификации на основании Пин-кода для входа в Мобильное приложение / Touch ID/ Face ID кода Клиента, Базовых Аутентификационных данных. С помощью Сессионного ключа осуществляется проверка подлинности ЭД, направляемых Клиентом в рамках Сеанса связи. По своей сути является простой электронной подписью.

1.32. Система «Интернет-банк» (Система) – автоматизированная информационная система дистанционного обслуживания Клиента через Официальный сайт или Мобильное приложение Банка с использованием сети Интернет.

1.33. Сторона/Стороны – Банк и Клиент/Банк или Клиент.

1.34. Тарифы – официальные документы Банка, устанавливающие размер и порядок оплаты комиссий, услуг Банка, а именно: «Тарифы комиссионных вознаграждений по обслуживанию банковских карт и счетов с использованием банковских карт АО КБ «Хлынов» и «Тарифы комиссионных вознаграждений на предоставляемое обслуживание физическим лицам в АО КБ

«Хлынов». Тарифы являются неотъемлемой частью Договора.

1.35. Транспортный пароль (Временный пароль) – пароль одноразового использования, используемый для Аутентификации Клиента при первом входе в Систему после проведения процедуры регистрации в Системе.

1.36. Финансовая платформа (финансовый маркетплейс) - информационная система которая обеспечивает взаимодействие Банка с Клиентом посредством информационно-телекоммуникационной сети "Интернет" в целях обеспечения возможности получения Клиентом услуг Банка и доступ к которой предоставляется оператором Финансовой платформы, с которым у Банка заключен договор.

1.37. Цифровой отпечаток – идентификатор устройства, сформированный в виде производного значения из значений параметров устройства, позволяющий идентифицировать устройство пользователя при получении им банковских и финансовых услуг.

1.38. Чат – сервис предоставления консультаций Клиентам, обратившимся через удаленный канал обслуживания и оказания некоторых услуг для авторизованных и неавторизованных пользователей Системы в часы работы, установленные Банком.

1.39. Электронный документ (ЭД) – документ, сформированный с использованием автоматизированных систем Банка и содержащий в электронной форме распоряжение Клиента Банку на совершение операций по Счетам Клиента или иных операций.

1.40. Face ID – технология Аутентификации с помощью сканера лица человека, встроенная в Мобильное устройство Клиента, инициируемая Мобильным приложением, посредством обращения к данной процедуре в устройстве для выполнения Аутентификации пользователя.

1.41. Push - уведомление – сообщение, отправляемое Банком с использованием сети Интернет на Мобильное устройство с установленным на нем Мобильным приложением и отображаемое на экране Мобильного устройства в виде всплывающего уведомления.

1.42. SMS-сообщения – текстовое сообщение, направляемое Банком на Номер мобильного телефона Клиента.

1.43. Touch ID – технология Аутентификации с помощью сканера отпечатков пальцев, встроенная в Мобильное устройство Клиента, инициируемая Мобильным приложением, посредством обращения к данной процедуре в устройстве для выполнения Аутентификации пользователя.

1.44. WEB-версия Системы «Интернет-Банк» («Банк Хлынов | Интернет-банк»**) –** возможность доступа к Системе «Интернет-банк» посредством браузера. Любые электронные документы, передаваемые через web-версию Системы «Интернет-Банк», а также действия, совершаемые посредством web-версии Системы «Интернет-Банк», имеют юридическую силу. Банк в любой момент по собственному усмотрению определяет и изменяет перечень банковских операций и функций, доступных в web-версии Системы «Интернет-Банк», а также устанавливает лимиты на суммы операций в web-версия Системы «Интернет-Банк».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Заявление, настоящие Условия, Тарифы, Руководство пользователя по Системе «Интернет-банк» Приложение 2 к Условиям(далее – Руководство пользователя), Правила безопасности Системы «Интернет-банк» Приложение 1 к Условиям (далее – Правила безопасности) в

совокупности являются Договором о предоставлении услуги «Интернет-банк» (далее – Договор), заключенным между Клиентом и Банком, и устанавливают правила и положения, регулирующие предоставление Банком услуги «Интернет-банк».

2.2. Банк оказывает Клиенту услугу «Интернет-банк» при наличии технической возможности в соответствии с Договором. Общий функционал Системы «Интернет-банк» включает в себя Информационный сервис и Платежный сервис. Клиент самостоятельно знакомится с функционалом Системы посредством Аутентификации и Авторизации, дальнейшей работы в Системе. Банк имеет право в одностороннем порядке изменить перечень услуг, оказываемых Клиенту в Системе «Интернет-банк».

2.3. Подключение к Системе осуществляется при наличии действующей Карты Банка (за исключением случаев, указанных в п. 2.4.4 и п. 2.4.5 настоящих Условий) и Номера мобильного телефона. Подключение к Системе не осуществляется по Карте, выпущенной на третье лицо, за исключением случая подключения к Системе финансового управляющего Клиента, утвержденного арбитражным судом в деле о банкротстве Клиента, а также корпоративной карте, выпущенной к корпоративному счету.

2.4. Доступ Клиента к Системе «Интернет-банк» осуществляется после выполнения процедур Идентификации, Аутентификации и Авторизации.

Заключение Договора осуществляется путем присоединения Клиента к Условиям в целом в соответствии со ст. 428 Гражданского кодекса Российской Федерации (далее – ГК РФ) и проводится предоставлением Клиентом в Банк Заявления, оформляемого по форме Банка и акцептом его Банком осуществляется одним из следующих способов: при личном обращении Клиента в офис Банка (при наличии данной услуги в офисе Банка), при регистрации через Официальный сайт Системы, при обращении Клиента через устройства самообслуживания Банка (при условии доступности услуги в устройстве), через Официальный сайт Банка и/или Мобильное приложение с использованием Единой Биометрической системы, через официальный сайт или мобильное приложение Финансовой платформы. Договор заключается на неопределенный срок.

Подключение Клиента к Системе возможно следующими способами:

2.4.1. через Официальный сайт Банка или Мобильное приложение Банка;

Заявлением признаётся самостоятельное подключение Клиента к Системе, которое осуществляется путём указания номера действующей Банковской карты Банка и серии/номера Паспорта гражданина РФ, Логин и Постоянный пароль формируются Клиентом самостоятельно. С целью подтверждения регистрации Банк направляет Клиенту Разовый код безопасности в виде SMS-сообщения на Номер мобильного телефона Клиента. При этом СМС-сообщение с информацией о Разовом коде безопасности является подтверждением принятия Заявления Банком, а ввод Клиентом Разового кода безопасности в подтверждение регистрации является подтверждением заключения Договора.

2.4.2. обращение Клиента в офис Банка:

Банк осуществляет подключение к Системе на основании подписанного Клиентом Заявления на подключении услуги «Интернет-банк». После подключения к Системе Банк направляет уведомление о подключении, уникальную сгенерированную Системой пару Логина и Транспортного пароля в виде SMS-сообщения на Номер мобильного телефона Клиента. При этом SMS-сообщение с уведомлением, Логином и Транспортным паролем являются подтверждением принятия Заявления Банком и заключения Договора.

2.4.3. в устройствах самообслуживания «Все просто»;

Заявлением признаётся самостоятельное подключение к Системе, которое осуществляется в личном кабинете устройства самообслуживания системы «Все просто», доступ к которому предоставляется при наличии действующей банковской карты и обязательном введении ПИН-кода. Информация о Логине выдается на чеке устройства самообслуживания, Транспортный пароль направляется Банком в виде SMS-сообщения на Номер мобильного телефона. Чек устройства самообслуживания с информацией об Идентификаторе пользователя и СМС-сообщение с Транспортным паролем в совокупности являются подтверждением принятия Заявления Банком и заключения Договора.

2.4.4. через Официальный сайт Банка или Мобильное приложение Банка с использованием Единой биометрической системы;

Заявлением признается самостоятельное подключение к Системе путем прохождения физическим лицом процедуры регистрации в системах Банка с предоставлением согласий на Едином портале государственных услуг и прохождения аутентификации с помощью Единой системы идентификации и аутентификации с использованием ранее сданных биометрических образцов. После предоставления необходимых данных для идентификации и приема физического лица на обслуживание Банку Клиент регистрируется в системах Банка. Клиенту направляется уведомление о подключении, уникальная сгенерированная Системой пара Логина и Транспортного пароля на Номер мобильного телефона Клиента. При этом SMS-сообщение с уведомлением, Логином и Транспортным паролем являются подтверждением принятия Заявления Банком и заключения Договора.

2.4.5. через официальный сайт или мобильное приложение Финансовой платформы;

Подключение к Системе осуществляется путем подписания Клиентом Заявления на подключение услуги Интернет-банк в личном кабинете на сайте Финансовой платформы. Данные, необходимые для идентификации Клиента собираются в соответствии с правилами Финансовой платформы и передаются в Банк по защищенным каналам связи для регистрации в системах Банка. Клиенту направляется уведомление о подключении, уникальная сгенерированная Системой пара Логина и Транспортного пароля на Номер мобильного телефона Клиента. При этом SMS-сообщение с уведомлением, Логином и Транспортным паролем являются подтверждением принятия Заявления Банком и заключения Договора.

2.5. При первом входе в Систему Транспортный пароль необходимо сменить на Постоянный пароль, руководствуясь рекомендациями Системы.

2.6. При подключении к Системе не может быть указан Логин, который уже используется в Системе.

2.7. Операции в Системе Клиент подтверждает Разовым кодом безопасности, который направляется ему в SMS сообщении на Номер мобильного телефона.

Необходимость подтверждения операции Разовым кодом безопасности определяет Банк и доводит данную информацию до Клиента путем ее отображения в Системе при совершении операции.

2.8. ЭД, созданный с использованием Системы и подписанный ПЭП, является документом, имеющим юридическую силу, равную аналогичным документам, оформленным в установленном порядке на бумажном носителе.

2.9. Клиент соглашается с получением услуги «Интернет-банк» через сеть Интернет, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести финансовые риски

и риски нарушения конфиденциальности, связанные с возможной Компрометацией информации при ее передаче через сеть Интернет. Рекомендации по безопасному использованию Системы приведены в Правилах безопасности.

2.10. Клиент самостоятельно и за свой счет обеспечивает подключение своего персонального компьютера и Мобильных устройств к сети Интернет, доступ к сети Интернет, а также обеспечивает защиту собственного персонального компьютера и своих Мобильных устройств от несанкционированного доступа и вредоносного программного обеспечения.

2.11. При проведении операций в Системе используется московское время.

2.12. Банк взимает с Клиента плату за совершение операций в Системе в соответствии с Тарифами Банка. Списание платы за совершение операций производится в соответствии с заранее данным акцептом/поручением Клиента со Счетов/вкладов Клиента, с которых производится списание средств по операциям.

2.13. Конвертация по операциям, принятым через Систему, осуществляется по курсу Банка, установленному на момент обработки принятого ЭД в автоматизированной банковской системе. Операции в Системе в иностранной валюте, а также по Счетам, открытым в иностранной валюте, осуществляются с учетом ограничений валютного законодательства Российской Федерации.

2.14. Клиент соглашается с тем, что Банк может направлять ему информацию об операциях по Счетам на адрес электронной почты, указанный Клиентом при формировании соответствующего запроса в Системе или определенный Клиентом в Заявлении на получение банковской карты.

2.15. Банк предоставляет информацию, связанную с использованием Системы, путем размещения настоящих Условий, Тарифов, Руководства пользователя и Правил безопасности на Официальном сайте Банка и/или на Официальном сайте Системы.

2.16. Обращения Клиентов, связанные с работой в Системе, принимаются по следующим каналам связи Банка:

-при личном визите в любой офис Банка;

-путем направления обращения по электронному адресу: callcenter@bank-hlynov.ru;

-путем обращения по многоканальному телефону единого сервисного центра: 8 (800) 250-2-777;

- путем обращения в Чат;

-путем направления письма по почте на адрес Банка, указанный в разделе 11.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Банк обязуется:

3.1.1. По запросу Клиента осуществить подключение к Системе в порядке и на условиях, установленных настоящими Условиями, предоставить Клиенту Логин и Транспортный пароль (если это предполагается способом подключения).

3.1.2. Принимать к исполнению поступившие от Клиента ЭД, оформленные в соответствии с действующим законодательством Российской Федерации, требованиями нормативных документов Банка России, настоящих Условий и договоров между Клиентом и Банком, подписанные ПЭП Клиента. Банк исполняет принятые ЭД не позднее рабочего дня, следующего за днем их

получения от Клиента.

3.1.3. Не разглашать и не передавать третьим лицам информацию о Клиенте и его операциях в Системе, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и настоящими Условиями.

3.1.4. Обеспечить сохранность обращений, направленных Клиенту и полученных от Клиента, и информации об операциях Клиента в Системе в течение срока, установленного действующим законодательством Российской Федерации.

3.1.5. Предоставить документы Клиенту по его запросу через Систему или на бумажном носителе в течение срока, установленного действующим законодательством Российской Федерации.

3.1.6. В случае временной невозможности предоставления доступа в Систему по техническим или иным причинам разместить на Официальном сайте Банка и/или на Официальном сайте Системы и/или в Системе соответствующую информацию.

3.1.7. Информировать Клиента о мерах информационной безопасности при использовании Системы, рисках Клиента и возможных последствиях для Клиента в случае несоблюдения мер информационной безопасности, рекомендованных Банком. Информирование осуществляется путем размещения Правил безопасности, а также иной информации на Официальном сайте Банка, на Официальном сайте Системы, при Аутентификации в Системе, в офисах Банка, путем отправки SMS-сообщений на Номер мобильного телефона или PUSH-уведомлений на Доверенное устройство Клиента.

3.1.8. При получении заявления Клиента блокировать Карту и/или доступ в Систему в связи с утратой Карты и/или ПИН-кода Карты, и/или Номера мобильного телефона, и/или Мобильного устройства, либо в связи с тем, что ПИН-код Карты и/или реквизиты Карты, и/или Разовый код безопасности, и/или Аутентификационные данные стали известны третьему лицу.

3.1.9. Уведомлять Клиента о приостановлении или прекращении использования Системы одним из следующих способов:

- при обращении Клиента в Единый сервисный центр. В таком случае информирование о приостановлении или прекращении использования Системы осуществляется сотрудником Единого сервисного центра в момент обращения Клиента, при этом уведомление считается исполненным Банком и полученным Клиентом;
- отправкой SMS - сообщения или PUSH - уведомлений на Номер мобильного телефона Клиента;
- отображением информационного сообщения в Системе.

При этом обязательство Банка по информированию Клиента о приостановлении или прекращении использования Системы путем направления Клиенту уведомления считается исполненным, а уведомление считается полученным Клиентом с момента направления Банком Клиенту соответствующего SMS - сообщения или PUSH - уведомлений, либо отображения Клиенту соответствующего информационного сообщения в Системе.

3.1.10. Обеспечить доступность Единого сервисного центра Банка по телефону 8(800)250-2-777 для взаимодействия с Клиентами по вопросам предоставления услуги «Интернет-банк» ежедневно с 7:30 до 23:00 по Московскому времени.

3.1.11. Рассмотреть претензии, связанные с использованием Системы, в срок не более 30 дней со дня получения заявления Клиента, а также не более 60 дней со дня получения заявления, в случае если оспариваемая операция носит характер трансграничного перевода денежных средств.

3.1.12. На основании обращения в Чат или письменного заявления Клиента, переданного в офис Банка, установить при наличии технической возможности ограничения по параметрам и типам операций, которые могут осуществляться Клиентом с использованием Системы в случаях и порядке, предусмотренных законодательством РФ.

3.2. Банк имеет право:

3.2.1. В одностороннем порядке прекратить предоставление услуги «Интернет-банк» Клиенту в случае нарушения Клиентом своих обязательств по Договору.

3.2.2. В соответствии с Условиями списывать со всех Счетов/вкладов Клиента, открытых в Банке, платы за услуги, предоставляемые посредством Системы в соответствии с Тарифами Банка.

3.2.3. Отказать Клиенту в проведении операции в случае отсутствия на Счетах Клиента средств для списания платы, достаточных для проведения операции с учетом возможных комиссий Банка, указания неправильных реквизитов получателя платежа/перевода, некорректное заполнение реквизитов, а также при наличии запретов или ограничений на проведение операций по Счетам в рамках законодательства, нормативных актов Банка России, Условий пользования банковскими картами или иного договора между сторонами, определяющего порядок проведения операций по соответствующим счетам.

3.2.4. Временно приостановить исполнение распоряжений, в т.ч. платежей Клиента при выявлении признаков совершения перевода денежных средств без согласия Клиента, а также при совпадении атрибутов получателя перевода с данными, полученными в рамках взаимодействия с АС "Фид-Антифрод" ФинЦЕРТ.

3.2.5. В случаях получения Банком от Банка России информации, содержащейся в базах данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, остановить исполнение распоряжений, в т.ч. платежей Клиента без возможности возобновления исполнения.

3.2.6. Временно, приостановить осуществление расходных операций со Счетов Клиента:

- при поступлении информации от Банка России о несанкционированных переводах в адрес Клиента;
- при поступлении информации из других источников о несанкционированных переводах в адрес Клиента.

3.2.7. В случае приостановки расходных операций со Счета Клиента, Банк:

- предоставляет Клиенту информацию о причинах блокировки и рекомендации по снижению рисков повторного осуществления перевода денежных средств без согласия Клиента;
- незамедлительно запрашивает у Клиента подтверждение возобновления исполнения распоряжения;
- при получении от Клиента подтверждения, возобновления исполнения распоряжений, Банк незамедлительно возобновляет исполнение распоряжений. При

неполучении от Клиента подтверждения возобновления исполнения распоряжения, Банк возобновляет исполнение распоряжения по истечении двух рабочих дней после дня совершения им действий, приведших к блокировке.

3.2.8. Устанавливать лимиты на совершение операций в Системе, а также реализовывать в Системе другие механизмы, снижающие риски Банка и Клиента.

3.2.9. Отказать Клиенту при рассмотрении его заявления в заключении договора на любой продукт Банка в случае неактуальности документов, предоставленных в Банк.

3.2.10. Требовать от Клиента предоставления документов и сведений, необходимых Банку для исполнения требований действующего законодательства Российской Федерации.

3.2.11. Приостановить или прекратить использование Системы Клиентом в следующих случаях:

- на срок до 2 рабочих дней предоставление доступа к Системе при выявлении фактов и признаков нарушения информационной безопасности, а также признаков осуществления перевода денежных средств без согласия Клиента, либо под воздействием третьих лиц, устанавливаемых Банком России и размещаемых на его официальном сайте в сети Интернет;

- по заявлению Клиента;

- при несвоевременном предоставлении Банку сведений (документов, в том числе удостоверяющих личность), предусмотренных Условиями, или иного нарушения Клиентом требований Условий;

- при наличии у Банка подозрений о том, что операции совершаются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, в соответствии с Федеральным законом от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- при превышении лимитов на совершение операций (включая временные лимиты совершения операций после смены пароля);

- в случае, если у Банка есть подозрения в компрометации Логина, Постоянного и/или Транспортного пароля, Пин-кода Мобильного приложения на Мобильном устройстве Клиента до момента получения подтверждения от Клиента совершаемых операций в соответствии с принятым в Банке порядком;

- при обращении Клиента с предоставлением информации, не соответствующей имеющейся информации о фактических операциях Клиента;

- при общении с Клиентом в Чате и невозможности с ним связаться с ним по телефону;

- при явном несоответствии индивидуальных признаков и образцов поведения Клиента при его обращении по телефону и невозможности устранить данные сомнения;

- в иных случаях, предусмотренных законодательством РФ.

3.2.12. Использовать предоставленные Клиентом, а также полученные из других официальных источников по защищенным каналам, в т.ч., но не ограничиваясь, Единой системы

межведомственного электронного взаимодействия (СМЭВ) данные Клиента, а также данные о движимом и недвижимом имуществе Клиента, прочих объектах, идентификаторы которых ранее присутствовали в распоряжениях, в т.ч. платежах Клиента с целью поиска, подсказки и отображения Клиенту в Системе информации о вновь получаемых уведомлениях о начислениях (обязательствах) от Государственной информационной системы о государственных и муниципальных платежах и Государственной информационной системы жилищно-коммунального хозяйства. Информация о найденных непогашенных обязательствах отображается в Системе при наличии технической возможности.

3.3. Банк не несет ответственность:

3.3.1. в случае невозможности предоставления доступа к Системе «Интернет-банк» по независящим от Банка обстоятельствам, в том числе по причине не предоставления Банку сторонними организациями, сервисов необходимых для предоставления услуги «Интернет-банк»;

3.3.2. за последствия несанкционированного доступа третьих лиц в Систему, компрометации Логина, Постоянного или Транспортного пароля, Разовых кодов безопасности, произошедших не по вине Банка;

3.3.3. в случаях необоснованного или ошибочного перечисления Клиентом средств получателям через Систему. Клиент самостоятельно управляет необходимым процессом возврата средств с их получателями;

3.3.4. за несвоевременное ознакомление Клиентом с получаемыми от Банка уведомлениями о проведенных операциях в Системе;

3.3.5. за несвоевременное ознакомление Клиентом с информацией о проводимых и планируемых технических работах на системах Банка, в том числе влияющих на доступность услуги «Интернет банк», а также с Правилами безопасности;

3.3.6. за операции, совершенные в Системе в случае утраты доступа Клиента к Системе или в случае использования Системы без согласия Клиента, в ситуациях случившихся не по вине Банка. При этом после момента получения Банком от Клиента надлежащего уведомления Банк предпринимает все возможные меры по минимизации потерь и рисков в связи с такой утратой;

3.3.7. за сбои в работе электронной почты, сети Интернет, сетей связи, операционных системах устройств Клиента, возникшие по независящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом уведомлений Банка/отчетов/информации по Карте/выписок/справок.

3.4. Клиент обязуется:

3.4.1. оплачивать комиссии Банку за банковские операции, осуществляемые с использованием услуги «Интернет-банк» в соответствии с Тарифами;

3.4.2. хранить в недоступном для третьих лиц месте и не передавать другим лицам свои Логин, Постоянный и Транспортный пароли, Разовые коды безопасности, ПИН-коды Карт, ПИН-код для быстрого входа в Мобильное приложение, необходимые для работы с Системой;

3.4.3. при Компрометации или подозрении на Компрометацию:

- Разового кода безопасности – незамедлительно произвести блокировку Карты и принять решение о ее перевыпуске, принять меры, направленные на предотвращение возможной Компрометации Разовых кодов безопасности на Мобильном устройстве Клиента;

– Логина/Постоянного пароля – незамедлительно произвести смену Логина/Постоянного пароля в Системе;

– Доверенного устройства – произвести удаление из списка доверенных устройств скомпрометированного устройства посредством функциональности Системы.

Незамедлительно уведомить Банк, обратившись в Единый сервисный центр Банка по телефону 8(800)-250-2-777 или любой офис Банка, но не позднее дня, следующего за днем получения от Банка SMS-сообщения и/или PUSH-уведомления о совершенной подозрительной операции или наступления факта/подозрения Компрометации.

3.4.4. перед вводом в Системе Разового кода безопасности или Транспортного пароля, полученного в SMS-сообщении, в обязательном порядке убедиться в том, что операция в Системе инициирована Клиентом. При наличии дополнительной информации в тексте SMS – сообщения о характере и/или параметрах операции Клиенту необходимо сверить реквизиты совершаемой операции с текстом SMS-сообщения, содержащим Разовый код безопасности/Транспортный пароль. Вводить Разовый код безопасности/Транспортный пароль в Систему следует только при условии согласия с проводимой операцией;

3.4.5. в случае изменения ранее представленных в Банк сведений Клиента (паспортных данных/данных иного документа, удостоверяющего личность, фамилии, имени, отчества, места жительства и других данных), своевременно уведомить Банк и предоставить документы и сведения, подтверждающие данные изменения;

3.4.6. предоставлять в Банк по первому требованию любые документы и сведения, необходимые Банку для осуществления функций, предусмотренных действующим законодательством Российской Федерации;

3.4.7. перед началом работы с Системой ознакомиться с Правилами безопасности, размещенными на Официальном сайте Банка и Официальном сайте Системы, а также неукоснительно их соблюдать в течение всего периода использования Системы;

3.4.8. не реже чем раз в месяц знакомиться с действующими Тарифами, Условиями и самостоятельно отслеживать их изменения, о которых Банк уведомляет путем публичного размещения информации на Официальном сайте Банка и Официальном сайте Системы;

3.4.9. уведомить Банк об утрате доступа к Системе или в случае использования Системы без согласия Клиента как можно скорее, но не позднее дня, следующего за днем получения Клиентом информации о совершении соответствующей операции. В целях информационного взаимодействия с Банком следует использовать только каналы связи, указанные в п. 2.16 Условий.

3.4.10. на постоянной основе осуществлять контроль операций, выполняемых посредством Системы.

3.5. Клиент имеет право:

3.5.1. осуществлять банковские операции с использованием Системы;

3.5.2. самостоятельно устанавливать ограничения максимальной суммы одной операции и (или) операций за определенный период времени, используя Систему или через обращение в Чат;

3.5.3. в случае возникновения претензий, связанных с предоставлением услуг с использованием Системы, Клиент может обратиться по каналам связи Банка, указанным в п. 2.16 настоящих Условий;

3.5.4. в случае необходимости обратиться в офис Банка для получения письменного подтверждения операции, произведенной в Системе, согласно Тарифам.

4. ПРЕДОСТАВЛЕНИЕ УВЕДОМЛЕНИЯ О СОВЕРШЕННЫХ ОПЕРАЦИЯХ. ПОРЯДОК ПРЕДЪЯВЛЕНИЯ ПРЕТЕНЗИЙ. БЛОКИРОВКА ДОСТУПА.

4.1. В соответствии с требованиями законодательства Российской Федерации Банк уведомляет Клиента об операциях, совершенных с использованием Карт Клиента и Системы, путем отражения информации об этих операциях в Мобильном приложении и/или WEB-версии Системы «Интернет-банк».

4.2. По платежам/переводам, совершенным с использованием Системы, Клиенту Системой предоставляется возможность формирования и печати платежного поручения или распоряжения на оплату.

4.3. Банком обеспечивается сохранность уведомлений, направленных Клиенту и полученных от Клиента, и информации об операциях Клиента в Системе в течение срока, установленного действующим законодательством Российской Федерации.

4.4. Клиент считается проинформированным об операциях по Картам Клиента и об операциях, совершенных посредством Системы, начиная с момента размещения/отображения информации о таких операциях в выписках по Счетам/Картам и/или истории совершенных операций в Системе.

4.5. В случае несогласия с операцией, отраженной в Системе, Клиент может обратиться в офис Банка с письменным заявлением, но не позднее дня, следующего за днем размещения информации в Системе. Срок рассмотрения заявления Клиента и информирование его о результатах рассмотрения не более 30 дней со дня получения заявления, а также не более 60 дней со дня получения заявления, в случае если оспариваемая операция носит характер трансграничного перевода денежных средств.

4.6. При утрате доступа к Системе или в случае использования Системы без согласия Клиента, Клиенту необходимо немедленно уведомить об этом Банк по телефонам: 8 (8332) 252-777, 8-800-250-2-777 (Единого сервисного центра Банка) для блокировки доступа к Системе или обратиться в офис Банка. Блокировка доступа Клиента к Системе производится Банком после проведения процедуры идентификации Клиента, при обращении по телефону (Банк может запросить дополнительную информацию) или после предъявления документа, удостоверяющего личность, при предоставлении соответствующего письменного заявления, оформляемого по форме Банка.

4.7. Приостановка возможности использования Клиентом Системы по устному обращению Клиента должна быть обязательно подтверждена в течение 5 (пяти) рабочих дней оформлением письменного заявления в офисе Банка. В случае невозможности явки Клиента в офис Банка, заявление, подписанное Клиентом, должно быть отправлено в адрес Банка: 610002, г. Киров, ул. Урицкого, 40. Указанные способы подтверждения ранее сделанного обращения (с учетом условий п. 4.4., 4.5.) считаются надлежащим уведомлением Банка Клиентом.

4.8. В случае ненадлежащего уведомления Банка об утрате доступа к Системе или использовании Системы без согласия Клиента, претензии Клиента по оспариваемым операциям не подлежат удовлетворению.

4.9. Для возобновления доступа к Системе, приостановленного по инициативе Клиента, Клиент предоставляет в Банк заявление о разблокировке доступа, оформляемого по форме Банка. При обращении Клиента в офис Банка все действия производятся при соблюдении процедуры Идентификации Клиента.

5. УСЛОВИЯ СОВЕРШЕНИЯ ОПЕРАЦИЙ

5.1. Перечень возможных получателей денежных переводов, осуществляющихся в рамках системы быстрых платежей (далее – СБП) ограничивается перечнем лиц, зарегистрированных в системе СБП. Правила, принципы и особенности работы с сервисами СБП описаны в «Правилах обслуживания клиентов АО КБ «Хлынов» с использованием Системы быстрых платежей» Приложение №3 к «Условиям пользования банковскими картами АО КБ «Хлынов», документ доступен на Официальном сайте Банка.

5.2. Осуществление переводов не ограниченно по времени и совпадает со временем доступности Системы.

5.3. Банк по своему усмотрению может ограничивать географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение Клиентом электронных сообщений, а также использованием Системы в целом.

5.4. Совершение переводов возможно с Доверенных устройств, зарегистрированных в Системе, путем ввода Клиентом Разового кода безопасности, отправленного на Номер мобильного телефона Клиента, в процессе прохождения дополнительной Аутентификации устройства.

5.5. Сумма перевода денежных средств с использованием Системы при переводе на Счета, открытые в Банке, не ограничена Системой (в том числе переводы на собственные счета, счета иных физических и юридических лиц).

5.6. Банк реализует комплекс мер по предотвращению операций проведенных без согласия Клиентов и минимизации прочих рисков, которые могут возникать при использовании по назначению Клиентом функциональности Системы. Комплекс мер разрабатывается, контролируется, актуализируется и доводится до сведения Клиента на усмотрение Банка, отражая соответствующую информацию в Тарифах. Такой комплекс мер может включать, не ограничиваясь, установление разовых, суточных, дневных, месячных и прочих лимитов по сумме и/или количеству операций и иных ограничений по параметрам операций при осуществлении операций с использованием Системы. При этом Клиент, создавая обращение в Чат или при обращении в офис Банка может запросить увеличение необходимого лимита.

5.7. Получателями денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием Системы, могут быть физические лица, юридические лица, индивидуальные предприниматели, самозанятые и государственные организации.

5.8. К устройствам, с использованием которых может осуществляться доступ к Системе, относятся: персональные компьютеры, мобильные телефоны, смартфоны, планшеты и прочие устройства, обладающие техническими параметрами, позволяющими использовать Систему, и доступом к сети Интернет.

5.9. Использование Системы может осуществляться круглосуточно при наличии доступа к сети Интернет, использование в автономном режиме не предусмотрено.

6. ПРОЧИЕ УСЛОВИЯ

6.1. В рамках предоставления услуги «Интернет-банк» для физических лиц Банк осуществляет

обработку персональных данных Пользователя Системы и иных лиц[1], которая непосредственно связана с исполнением заключаемого договора, в частности в рамках:

- получения справочной информации о состоянии счетов и остатке задолженности по кредитным договорам;
- осуществления переводов и платежей;
- получения услуг Банка по оформлению Карт, Счетов, вкладов, кредитных продуктов;
- просмотра заявлений, анкет, договоров, заключенных в электронном виде;
- актуализации паспортных данных;
- использования сервиса предоставления консультаций Клиентам (Чат)
- автоматического поиска налогов, штрафов, счетов и оплаты начислений;
- оформления страховых продуктов

для чего Банк может обрабатывать персональные данные Пользователя Системы, а также иных лиц в зависимости от выбранного функционала Системы, а именно: фамилию, имя, отчество, дату, месяц, год рождения, мобильный телефон, адрес регистрации, адрес проживания, адрес электронной почты, паспортные данные, в том числе скан-копию документа, вид на жительство в РФ, временное удостоверение личности гражданина РФ, миграционную карту, паспорт иностранного гражданина или удостоверение личности лица без гражданства, паспорт моряка, разрешение на временное проживание, свидетельство о рождении, справку об освобождении из мест лишения свободы, удостоверение беженца, удостоверение личности военнослужащего РФ, ИНН, СНИЛС, водительское удостоверение, свидетельство о регистрации транспортного средства, УИН ГИС ГМП/ИС РНиП, сведения о состоянии счетов, сведения о доходах и расходах, включая сведения о задолженности по кредитным договорам, реквизиты счета, номер карты, образование, семейное положение (фамилия, имя, отчество супруга/супруги, дата, месяц, год рождения супруга/супруги), место работы, должность, а также иную доступную либо предоставленную Пользователем Системы информацию в рамках эксплуатации Системы.

Обработка персональных данных Пользователя Системы, а также иных лиц включает в себя совершение любых действий (операций) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), блокирование, удаление, уничтожение и ограничивается сроком использования Пользователем системы функционала Системы «Интернет-банк», если иное не предусмотрено Договором.

Заключая с Банком Договор о предоставлении услуги «Интернет-банк» путем присоединения Клиента к Условиям, Тарифам, Руководству пользователя, Правилам безопасности Пользователь Системы соглашается с получением рекламных материалов, сообщений и предложений АО КБ «Хлынов» и Партнеров, предложения о товарах и услугах которых размещены в Системе, в том числе посредством push-уведомлений. В случае, если Пользователь не желает получать

[1] Лица, в отношении которых могут совершаться платежи и переводы, оплата услуг, а также оформление услуг Банка и партнеров, включая страховых продуктов: получатели денежных средств, выгодоприобретатели по договору страхования.

перечисленную выше информацию, он вправе обратиться с просьбой об отмене направления в его адрес рекламных сообщений любым удобным способом, позволяющим идентифицировать обращающееся лицо.

В случае предоставления персональных данных третьих лиц, Пользователь подтверждает, что им получены согласия таких лиц на обработку их персональных данных или наличие у него полномочий на выражение согласия от имени таких лиц и что такие лица уведомлены об осуществлении обработки персональных данных Банком, а также обязуется по запросу Банка незамедлительно предоставить информацию и документы, подтверждающие правомерность передачи в Банк персональных данных третьих лиц, в том числе согласия на обработку персональных данных.

6.2. За невыполнение или ненадлежащее выполнение обязательств по настоящим Условиям Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

6.3. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Банком своих функций по настоящим Условиям, и иных обстоятельств, не зависящих от Банка, Банк освобождается от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

6.4. Банк освобождается от имущественной ответственности в случае технических сбоев (отключение/повреждение электропитания и сетей связи, сбой программного обеспечения процессингового центра и баз данных Банка, технические сбои в платежных системах и т.п.). Обязательства Банка по настоящим Условиям считаются прекращенными с даты прекращения обязательств Банка по договорам и дополнительным соглашениям к ним по Счетам Клиента, указанным в Заявлении о блокировке доступа к системе «Интернет-банк».

6.5. Банк уделяет повышенное внимание противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ) и реализует совокупность мер, направленных на ПОД/ФТ/ФРОМУ. Банк в своей деятельности руководствуется Федеральным законом от 07.08.2001 N115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

7. ОБЩИЕ УСЛОВИЯ ОБМЕНА ЭД С ИСПОЛЬЗОВАНИЕМ ПЭП МЕЖДУ БАНКОМ И КЛИЕНТОМ

7.1. Настоящий раздел определяет общие условия обмена ЭД с использованием ПЭП между Банком и Клиентом.

7.2. Банк и Клиент договорились об использовании между ними ПЭП для:

– совершения любых банковских операций в соответствии с действующим законодательством;

– заключения и исполнения любых гражданско-правовых сделок с Банком, если специальный порядок заключения, изменения, расторжения не предусмотрен законодательством Российской Федерации и настоящими Условиями;

– передачи в Банк любых заявлений и сообщений;

– обмена с Банком любой информацией;

– формирования неограниченного количества ПЭП для подписания расчетных и иных документов в отношении любых Счетов, в том числе и вновь открываемых;

– достижения договоренностей с Банком об использовании новых ПЭП любого вида;

– совершения иных юридически значимых действий, направленных на исполнение обязательств, установление, изменение или прекращение правоотношений с Банком;

– обмена информацией и документами, совершения юридически значимых действий, направленных на исполнение обязательств, установление или прекращение правоотношений между Клиентами.

7.3. ЭД порождает обязательства, если передающей стороной он надлежащим образом оформлен, заверен ПЭП, подтвержден и передан, а принимающей стороной получен, проверен и принят.

7.4. ЭД Клиента, созданный с использованием Системы и подписанный ПЭП, переданный посредством Системы и полученный Банком, является документом, имеющим юридическую силу, равную аналогичным документам надлежащим образом, оформленным на бумажных носителях, подписанным собственноручными подписями.

7.5. Действия, совершенные Банком, а также сделки, заключенные между Клиентом и Банком на основании ЭД, не могут быть оспорены только на том основании, что эти действия не подтверждаются документами, составленными на бумажных носителях.

7.6. Банк вправе в любой момент потребовать от Клиента подписания, а Клиент обязан по требованию Банка подписать ранее переданные Банку ЭД на бумажном носителе, независимо от того, исполнены ли указанные ЭД.

7.7. В случае передачи Клиентом Банку ЭД, подписанного ПЭП, с вложениями, вложения считаются также подписанными ПЭП и являются эквивалентными подобным документам, составленным на бумажных носителях, и влекут аналогичные документам, составленным на бумажном носителе, права и обязанности Сторон.

7.8. Банк не несет ответственности в случае, если информация о Счетах Клиента, сведения о Клиенте и/или операциях по Счету/Счетам Клиента станет известна третьим лицам в результате использования Клиентом незашифрованных каналов связи для доступа к сети Интернет, используемых Клиентом для доступа к дистанционному банковскому обслуживанию, и/или в результате прослушивания и/или перехвата каналов связи для доступа к сети Интернет, используемых Клиентом для доступа к дистанционному банковскому обслуживанию.

7.9. Банк и Клиент признают в качестве единой шкалы времени при работе в Системе Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

7.10. ЭД считается переданным Клиентом, если выполнены все этапы нижеследующей процедуры передачи ЭД:

– Идентификация, Аутентификация и Авторизация входа Клиента в Систему прошла

успешно;

– Клиент ввел/сообщил содержание ЭД и его параметры;

– Клиент подтвердил правильность ввода ЭД и его параметров, выбрав команду на совершение соответствующего действия/ подписания соответствующего документа.

7.11. Считается, что Клиент отказался от передачи ЭД, если он не подтвердил правильность ввода ЭД и его параметров.

7.12. При использовании ПЭП при обмене ЭД Банк и Клиент признают, что:

– недопустимо внесение Клиентом изменений в ЭД после его подписания ПЭП;

– при возникновении спора о соблюдении правил обмена ЭД эталоном является журнал обмена ЭД хранящиеся на сервере Банка.

7.13. ЭД Клиентов принимаются круглосуточно. ЭД исполняется Банком не позднее следующего рабочего дня с даты его принятия Банком.

7.14. Банк отказывает в регистрации ЭД или в выполнении ранее переданного Клиентом и зарегистрированного Банком ЭД, если в процессе регистрации или после регистрации распоряжения выясняется, что:

– имеется информация, свидетельствующая о возможном нарушении Клиентом Договора или выяснено, что переданный Клиентом ЭД полностью или в части противоречит действующему законодательству Российской Федерации или Договору;

– в иных случаях, предусмотренных Договором.

7.15. В случае отказа от выполнения ранее переданного и зарегистрированного Банком ЭД, Банк оповещает Клиента о причинах такого отказа через Чат Системы или звонком на Номер мобильного телефона Клиента.

7.16. Для отмены ранее переданного ЭД Клиент вправе позвонить в Банк на соответствующий номер телефона Единого сервисного центра Банка по телефону 8 (800) 250-2-777 (звонок по России бесплатный), совершить соответствующие действия посредством Системы или Мобильного приложения .В случае неполучения Разового кода безопасности в SMS-сообщении при необходимости дополнительного подтверждения совершаемого в Системе действия, Клиент обязан обратиться в Единый сервисный центр или офис Банка для выяснения причин.

7.17. Клиент понимает и соглашается с тем, что использование Клиентом Системы возможно лишь согласно предоставленному Банком в любой момент в течение срока действия Договора комплексу функционала, информационного наполнения, интерфейса, дизайна, иных составляющих и условий использования Системы.

7.18. Изменение порядка работы, в том числе интерфейса, дизайна, информационного наполнения, функционала и любых составляющих Системы по волеизъявлению Клиента технически невозможно, что не является ненадлежащим исполнением Банком Условий и нарушением Банком прав и законных интересов Клиента.

7.19. Отзыв Клиентом согласия на обработку персональных данных также не является основанием для внесения Банком каких-либо изменений в порядок работы Системы, поскольку обработка Банком персональных данных Клиента в рамках функционирования Системы связана

исключительно с исполнением условий Договора.

8. УСЛУГА «ЧАТ»

8.1. Клиент имеет возможность вести электронную переписку с Банком посредством сервиса «Чат». Банк и Клиент договорились, что любая переписка между Банком и Клиентом посредством сервиса «Чат» после прохождения Идентификации и Аутентификации Клиента в Системе считается обменом ЭД, подписанными ПЭП Клиента. Такая переписка является юридически значимой, как если бы она осуществлялась на бумажных носителях с подписью уполномоченных лиц.

8.2. Каждое сообщение Клиента передается вместе с Сессионным ключом, который проверяется на корректность.

8.3. Если из переписки в Чате Банк установит волеизъявление Клиента, Банк может сформировать и направить на исполнение ЭД от имени Клиента в случае его подтверждения. При этом Клиент несет ответственность за передачу Банку правильных и достаточных реквизитов для совершения перевода, формирование и содержание запроса или сообщения Банку. Аналогом собственноручной подписи Клиента, используемым для подписания ЭД в Системе, является подтверждение на совершение операции (отправка в Банк сообщения, текст которого Клиент самостоятельно вводит, выражая согласие на проведение соответствующей операции).

8.4. Клиент обязан вести переписку посредством сервиса «Чат» в корректной форме, без использования оскорбительных и нецензурных выражений, непристойных фраз и бранных слов, а также соблюдать все общепринятые морально-этические нормы общения. В случае неисполнения Клиентом обязанности, предусмотренной настоящим пунктом, Банк вправе уведомить Клиента о недопустимости ведения дальнейшей переписки в некорректной форме.

8.5. Ограничение доступности сервиса «Чат» не влечет за собой наложения каких-либо иных ограничений на использование Клиентом любых других функций, сервисов и услуг Системы, доступных для Клиента, кроме возможности ведения переписки с Банком посредством сервиса «Чат».

9. УТВЕРЖДЕНИЕ УСЛОВИЙ И ТАРИФОВ, ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА

9.1. В соответствии с п. 1 ст. 450 ГК РФ Стороны договорились, что Банк имеет право вносить изменения в Условия и/или Тарифы. Банк доводит до сведения Клиента информацию об изменениях в любой из форм, предусмотренных п.9.2 Условий. Доведение указанной информации до сведения Клиента является адресованной Клиенту офертой Банка об изменении и/или дополнении Условий и/или Тарифов. Датой ввода в действие Условий и/или Тарифов в измененной и/или дополненной редакции является первый рабочий день календарного месяца, следующего за календарным месяцем, в котором Банк довел до сведения Клиента соответствующую информацию.

Клиент может акцептовать (принять) оферту (предложение) Банка об изменении и/или дополнении Условий и/или Тарифов путём предоставления в Банк письменного заявления о согласии с офертой Банка не позднее даты ввода в действие Условий и/или Тарифов в измененной и/или дополненной редакции.

Клиент может отказаться от акцепта оферты (предложения) Банка об изменении и/или дополнении Условий не позднее даты ввода в действие Условий и/или Тарифов в измененной и/или дополненной редакции путём предоставления в Банк письменное заявление о несогласии с

офертой Банка с указанием на согласие обслуживаться на ранее согласованных Сторонами условиях, либо письменное заявление о расторжении Договора.

Если до даты ввода в действие Условий и/или Тарифов в изменённой и/или дополненной редакции Клиент, способами, указанными выше, не акцептует (не примет) оферту (предложение) Банка либо не откажется от акцепта оферты Банка или не заявит о расторжении Условий и/или Тарифов, то такое молчание Клиента является акцептом Клиентом оферты Банка и по истечении указанного выше срока Условий и/или Тарифов считаются измененными по соглашению Сторон.

9.2. Информацию об изменении и/или дополнении Условий и/или Тарифов Банк доводит до сведения Клиентов не позднее, чем за 10 (десять) календарных дней до даты ввода вносимых изменений и дополнений в действие путём опубликования соответствующей информации с полным текстом изменений на Официальном сайте Банка.

Информирование Клиента дополнительно может сопровождаться рассылкой сообщений по электронным средствам связи, или производиться любыми иными способами по усмотрению Банка.
Датой ознакомления Клиента с доведённой до его сведения информацией и/или дополнении Условий и/или Тарифов Банка считается дата опубликования соответствующей информации.

9.3. Договор может быть в любое время расторгнут Клиентом при условии отсутствия нарушений со стороны Клиента, в том числе в случае несогласия Клиента с Условиями и/или Тарифами Банка.

9.4. Банк вправе расторгнуть Договор с Клиентом по основаниям, предусмотренным законодательством Российской Федерации.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Вопросы / правоотношения, не урегулированные Договором, разрешаются в соответствии с действующим законодательством Российской Федерации.

10.2. Положения Договора, в том числе Правила безопасности и Тарифы, применяются к правоотношениям сторон в части, не противоречащей законодательству Российской Федерации, в том числе ГК РФ, нормативным актам Банка России.

10.3. Любые вопросы, споры и разногласия, возникающие из Договора или в связи с ним, могут быть урегулированы сторонами путем переговоров. В случае, если Стороны не достигли согласия, споры подлежат разрешению в судебном порядке в соответствии с действующим законодательством Российской Федерации.

10.4. Уведомления, извещения, иная корреспонденция, если иное не предусмотрено условиями Договора, направляются:

– Банком по адресу места жительства или месту пребывания Клиента, указанному в Договоре, либо вручаются лично в руки при явке Клиента в Банк;

– Клиентом – по адресу Банка, указанному в Договоре, либо вручаются под расписку.

В случае направления указанных документов Банком по почте заказным письмом датой его получения считается четырнадцатый день со дня отправки заказного письма.

10.5. Подписание Клиентом Договора свидетельствует о том, что Клиенту была предоставлена исчерпывающая информация о предоставляемых ему услугах и полностью разъяснены все

вопросы, имеющиеся у него по Договору.

11. ЮРИДИЧЕСКИЙ АДРЕС И РЕКВИЗИТЫ БАНКА

Коммерческий банк «Хлынов» (акционерное общество)

610002, Российская Федерация, г. Киров (областной), ул. Урицкого, 40,

ИНН 4346013603, ОГРН 1024300000042, БИК 043304711,

Корреспондентский счет N30101810100000000711 в Отделении по Кировской области Волго-Вятского главного управления Центрального банка Российской Федерации.

Тел.: (8332) 252-777 факс: (8332) 252-504.

12. ИНФОРМАЦИЯ О НАИМЕНОВАНИИ, МЕСТЕ НАХОЖДЕНИЯ ПОСТАВЩИКА ПЛАТЕЖНОГО ПРИЛОЖЕНИЯ.

Система функционирует на базе программного обеспечения iSimpleLab разработчика программного продукта ООО «АйСимплЛаб» (г. Москва, ИНН 7704799375) (далее – Разработчик).

Разработчиком, помимо работ по развитию и доработке Системы, проводятся испытания Системы в средах ее функционирования, выполняемые в рамках проведения оценки соответствия требованиям ГОСТ Р ИСО/МЭК 15308-3-2013 и Профиля защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций.

Приложение 1 к Условиям
предоставления услуги «Интернет-банк»
физическим лицам

Правила безопасности Системы «Интернет-банк»

Термины, используемые в настоящих Правилах, имеют то же значение, что и в Условиях.

Вход и регистрация

1. Для входа в Систему «Интернет-банк» нужны: логин, пароль и уникальный код из SMS-сообщения, которое приходит на ваш номер телефона при первом входе или авторизации с нового устройства. Никому и никогда не передавайте эти данные, даже сотрудникам Банка и специальным органам.
2. В случае, если на странице Вас просят ввести любую другую персональную информацию, например, Номер мобильного телефона, ИНН или прочие личные данные, не выполняйте никаких операций и свяжитесь с сотрудниками Банка по номеру телефона Единого сервисного центра 8 800 250 2 777.
3. Полный номер вашей банковской карты и также паспортные данные требуются только для процедуры регистрации и восстановления доступа.

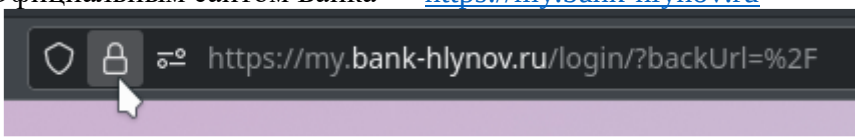
4. Сотрудники Банка никогда не попросят вас установить какое-либо дополнительное приложение для помощи или решения вопроса, кроме самого официального приложения Интернет-банка.

Коды в SMS-сообщениях

1. Никому не говорите Ваш пароль и Разовый код безопасности операции. Если Разовый код безопасности можно сообщить менеджеру — мы сразу напишем это в SMS-сообщении с кодом.
2. Сотрудники Банка никогда не просят сообщить данные учетной записи или коды подтверждения операций перевода.
3. Банк никогда не отправляет коды подтверждения для отмены операций. Все направляемые вам коды – это коды подтверждения операции. Если сомневаетесь, то для отмены операции достаточно никуда не передавать такой код.
4. Внимательно проверяйте параметры операции в SMS-сообщении, содержащем Разовый код безопасности. Информация в нем должна совпадать с вашей операцией в Системе «Интернет-банк», которую вы хотите подтвердить. Если эта информация не совпадает, не вводите Разовый код безопасности и сообщите об этом сотрудниками Банка по телефону Единого сервисного центра 8 800 250 2 777.
5. Отключите отображение текста SMS-сообщения на экране смартфона или смарт-часов, установите код для его разблокировки, даже для кнопочного телефона. Это позволит сохранить в тайне от злоумышленников коды подтверждения операций.

Общие рекомендации

1. Установите и обновляйте антивирус на вашем компьютере. Желательно использовать антивирусные программы и на мобильных устройствах.
2. Никогда не устанавливайте на телефон приложения из недостоверных источников.
3. Не устанавливайте на смартфон и компьютер программы для удаленного управления устройством.
4. Своевременно устанавливайте обновления операционной системы своего компьютера и мобильного устройства.
5. При входе в Систему «Интернет-банк» убедитесь, что установлено защищенное соединение именно с Официальным сайтом Банка — https://my.bank-hlynov.ru



6. Если у Вас есть подозрения, что кто-либо использует Ваш пароль или исполняются операции, которые Вы не совершали, незамедлительно обратитесь в Банк, например, по вышеуказанному телефону Единого сервисного центра.
7. Все сообщения об активности мошенников важны. Банк использует их для пресечения деятельности мошенников. Ваша активная позиция помогает нам в этом.
8. Не подключайте к общедоступным беспроводным сетям (Wi-Fi) во время работы с банковскими и государственными сайтами/мобильными приложениями (Интернет-Банки, Госуслуги, Личный кабинет налоговой и прочее). Ведь даже в других ситуациях их использование небезопасно. Через них злоумышленники могут скопировать введенные вами конфиденциальные данные, как минимум логин и пароль.

Как придумать надежный логин и пароль?

Хороший пароль состоит из заглавных и строчных букв, цифр и знаков препинания. Чем длиннее пароль, тем сложнее его подобрать. Рекомендуем придумывать пароли не менее 8 знаков. Например, так может выглядеть надежный пароль длиной в 16 знаков — jcX5C1%vj-AyuMaR. Такие пароли невозможно подобрать с помощью словаря, а на перебор уйдут месяцы и годы.

Как запомнить пароль?

Лучше всего пароль запоминается тогда, когда вы его часто вводите. Если вы только придумали пароль, отключите галочку «запомнить меня», и вам придется вводить его каждый раз при входе в Систему «Интернет-банк». Так ваши руки научатся вводить его автоматически.

Специалисты по безопасности не советуют записывать пароли в открытом виде, даже если вы будете держать их в сейфе. Если вам необходимо записать пароль, сделайте это так, чтобы только вы знали, как его прочитать.

Ни в коем случае не держите пароли на стикерах на мониторе. Не носите их в бумажнике. Не записывайте в заметки в телефоне.

Как не рассекретить пароль?

1. Используйте правило: один ресурс — один пароль. Не устанавливайте одинаковые пароли на социальные сети, электронные ящики, и, тем более, банковские аккаунты.
2. Постарайтесь использовать двухфакторную авторизацию везде, где это возможно. Работает это очень просто: при каждом новом входе ресурс будет запрашивать у вас код из SMS-сообщения. А так как телефон всегда рядом с вами - мошенники до него просто так не доберутся.
3. По возможности, не вводите пароли на чужих компьютерах и мобильных устройствах. Особенно, если эти компьютеры находятся в публичной зоне использования: интернет-кафе, площадки на фуд-кортах, игровые клубы, библиотеки. Если все-таки пришлось, проверьте, чтобы функция «запоминания» вводимых данных была неактивна, а по окончании сеанса использования сайта/мобильного приложения найдите функцию «выхода» из учетной записи и воспользуйтесь ею. Не лишним будет сменить пароль.
4. Надежно защитите сложным паролем домашнюю беспроводную сеть.
5. Если беда произошла и ваш пароль попал в руки к мошенникам - меняйте его на новый только в безопасной среде. Например, только дома и только с того устройства, которое является лично вашим.
6. Обязательно установите PIN-код на свою SIM-карту. Любой современный оператор мобильной связи позволяет устанавливать такой код. Обычно, PIN можно установить в разделе настроек SIM-карты.
7. Не используйте простые пароли и легкие графические ключи на своем мобильном устройстве.
8. При потере мобильного телефона, на который Вы получаете SMS-сообщения с разовым кодом безопасности, сразу же обратитесь к оператору мобильной связи и заблокируйте SIM-карту. В случае утраты банковской карты, заблокируйте ее через Официальный Сайт Банка/Мобильное приложение Банка и/или уведомите Банк по телефону.

Приложение 2 к Условиям
предоставления услуги «Интернет-банк»
физическим лицам

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 Официальным сайт Банка или Мобильном приложение 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 приложение Финансовой платформы.

3. Разовый код безопасности

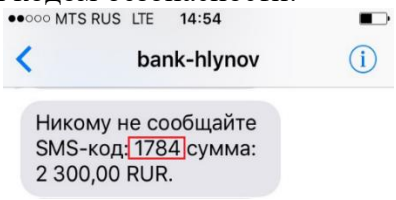
Разовый код безопасности используется для дополнительной Аутентификации пользователя при совершении операций в Системе.

> **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.

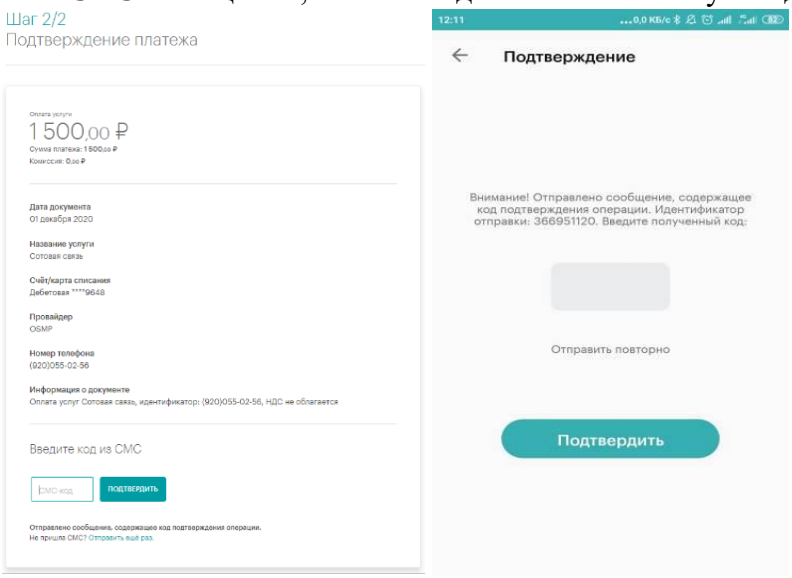
Пример SMS-сообщения с Разовым кодом безопасности:



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»:



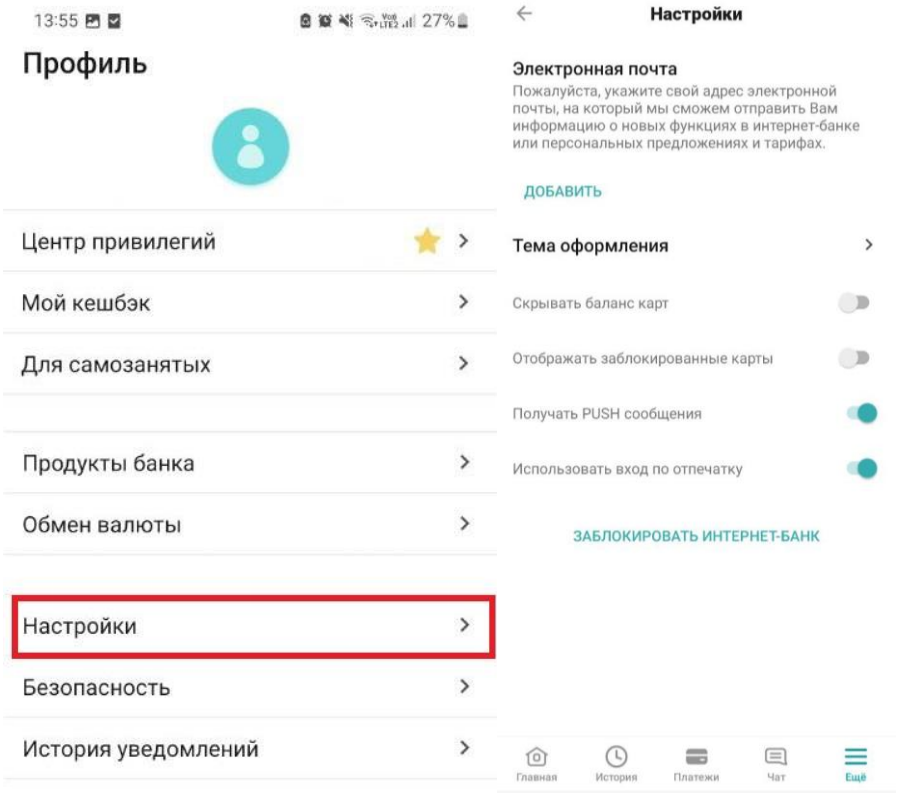
5. Push-уведомление

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 нестабильны 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;

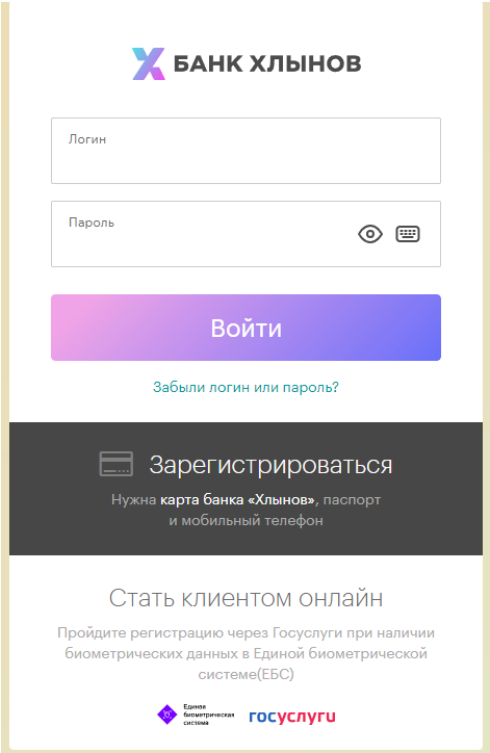
– может содержать элементы пунктуации из списка: «!», «@», «#», «$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «:», «;», «,», «.» (иные элементы пунктуации, в том числе пробел, не допустимы).

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.

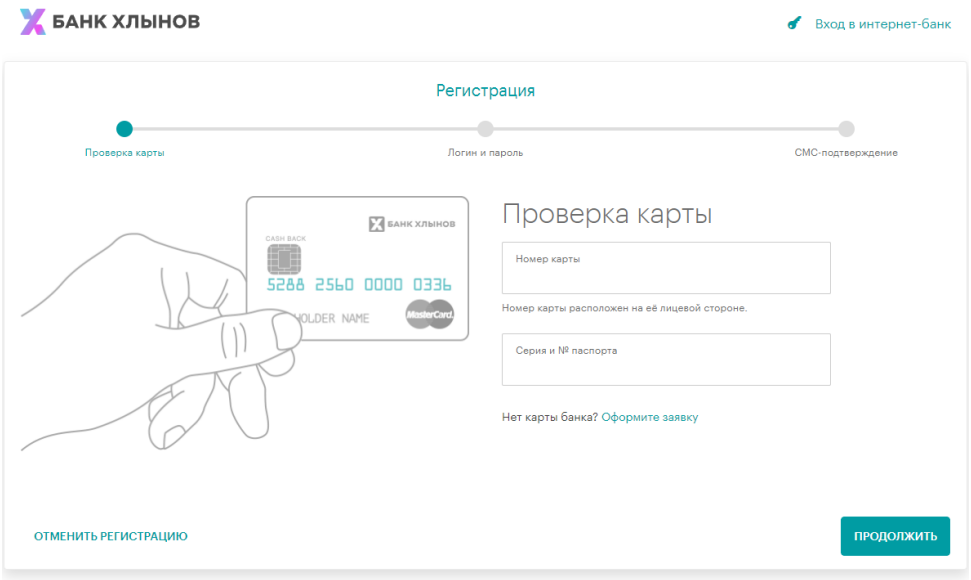
6.1. Регистрация в Системе на Официальном сайте Банка

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.



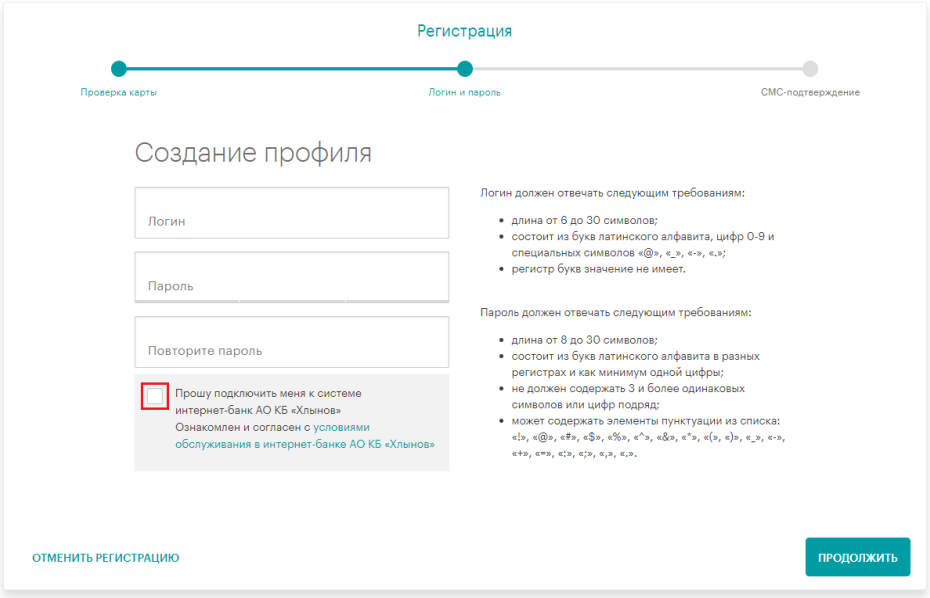
На открывшейся странице необходимо заполнить следующие данные: номер действующей основной Карты, который изображен на ее лицевой стороне (16 цифр), номер документа, удостоверяющего личность.



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

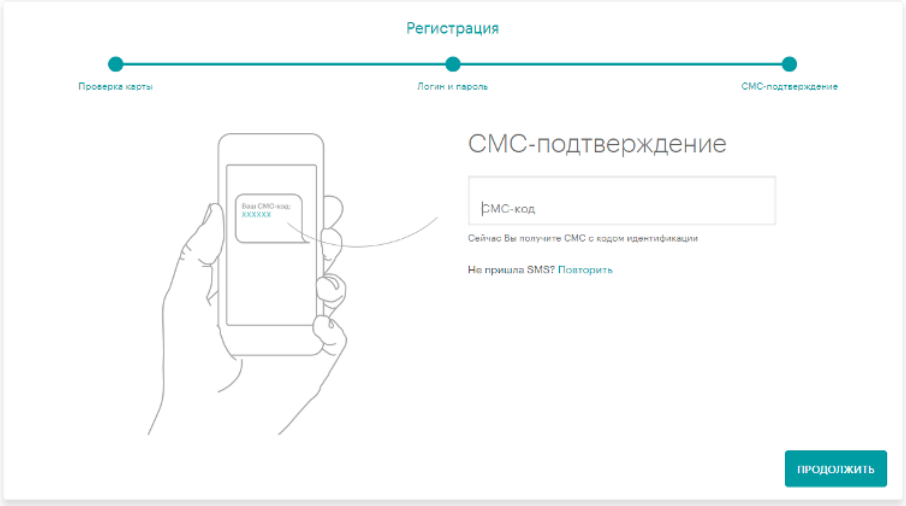
В появившемся окне **«Создание профиля»** нужно указать желаемые Логин и Пароль (необходимо повторить ввод Пароля в поле «Повторить пароль»).

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».

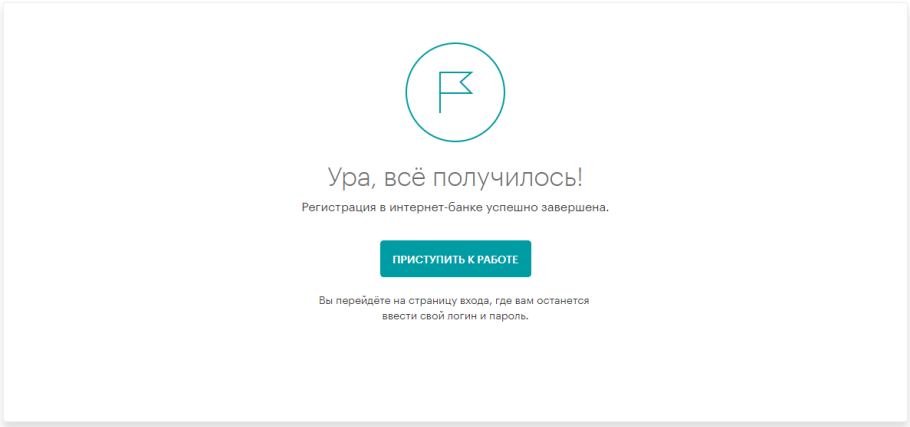


При успешной регистрации в Системе по кнопке «**Продолжить»** необходимо перейти на

окончательный этап регистрации **«SMS-подтверждение»**.

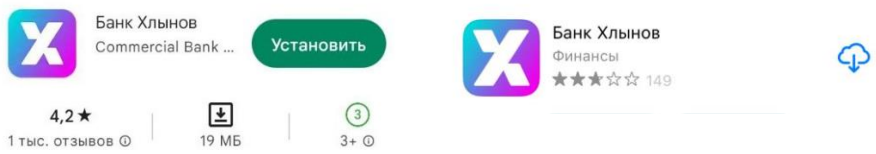


На привязанный к Карте Номер мобильного телефона придет Разовый код безопасности. После ввода кода из SMS-сообщения регистрация в Системе «Интернет-банк» будет завершена и можно приступить к работе.

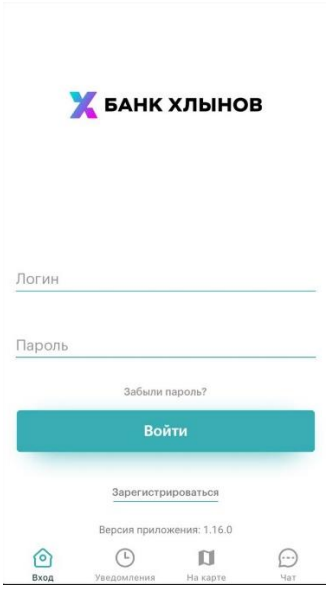


6.2. Регистрация через Мобильное приложение

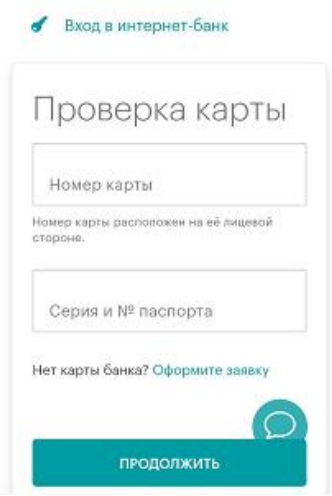
Для начала работы с мобильной версией Системы необходимо в сервисе Google Play Market, Apple Store, Huawei AppGallery, RuStore скачать на Мобильное устройство Мобильное приложение «**Банк Хлынов**». (*Системные требования для корректной работы Приложения: ОС Android 5.0 и выше, iOS 13 и выше)*



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.



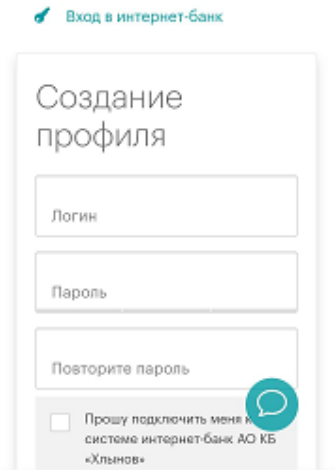
На открывшейся странице проверки Карты необходимо заполнить следующие данные: номер действующей основной Карты, который изображен на ее лицевой стороне (16 цифр), номер документа, удостоверяющего личность.



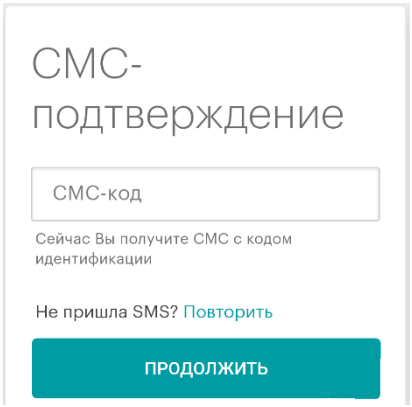
После ввода номера Карты и реквизитов документа, удостоверяющего личность, продолжить процесс регистрации нажатием на «**Продолжить».**

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

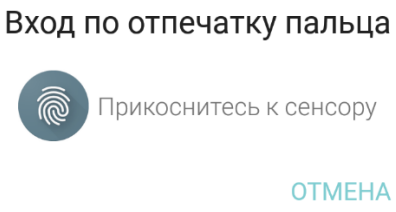
После создания Логина и Пароля необходимо ознакомиться с Условиями обслуживания в интернет-банке АО КБ «Хлынов» и отметить пункт «Прошу подключить меня к системе интернет-банк АО КБ «Хлынов», ознакомлен и согласен с Условиями обслуживания в интернет-банк АО КБ «Хлынов».



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



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.



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»**).

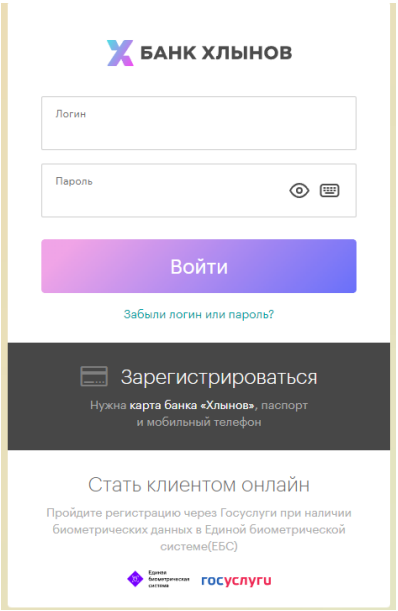
Обратите внимание! Если вход в Систему осуществляется с нового устройства Клиента или используется другой состав программного обеспечения такого устройства, то для такого входа могут быть запрошены дополнительные данные, в частности Разовый код безопасности. После ввода кода из соответствующего SMS-сообщения 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.

a. **На Официальном сайте Банка**

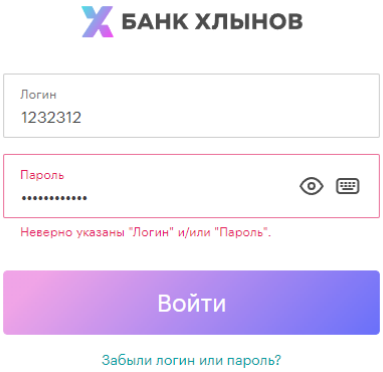
Зайдите на Официальный сайт Банка (https://www.bank-hlynov.ru/), в верхней правой части страницы из выпадающего меню **«Интернет-банк»** выберите раздел **«Частным клиентам»**

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»**.

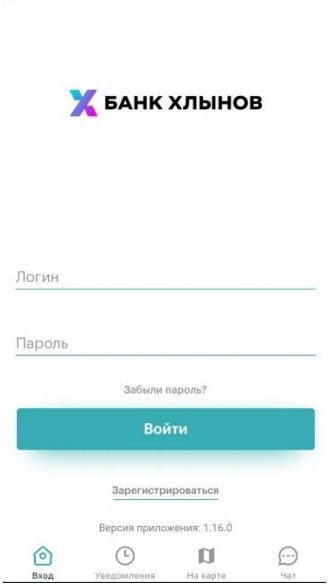


Если поле Логин или Пароль заполнены неверно, появится соответствующая всплывающая подсказка.

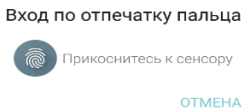


b. **С использованием Мобильного приложения**

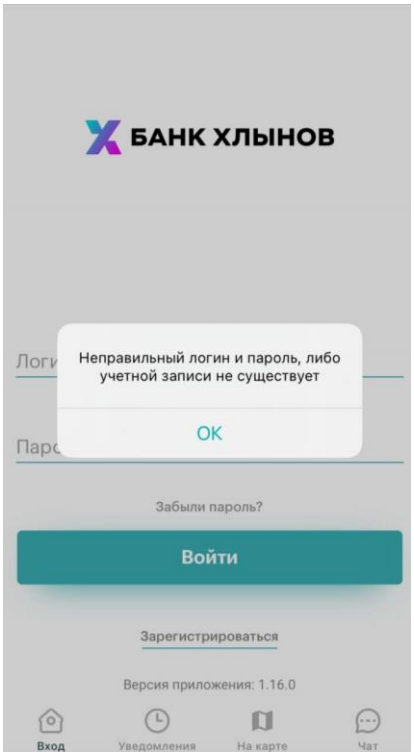
Для входа в Систему введите Логин и Пароль в соответствующие поля, а затем нажмите кнопку «**Войти**».



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.



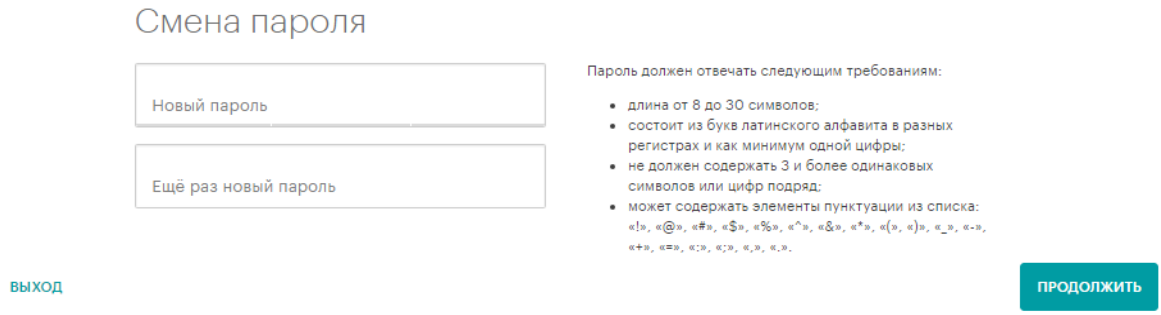
Если поле Логин или Пароль заполнены неверно, появится соответствующая всплывающая подсказка.



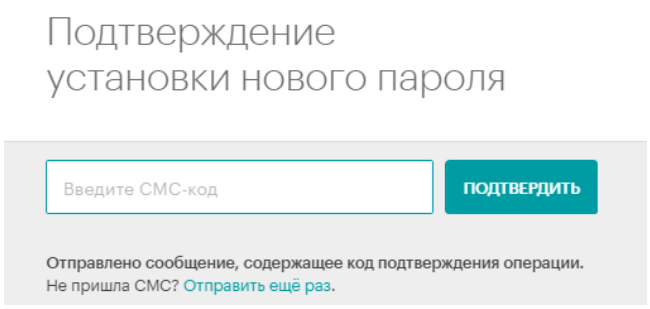
8. Изменение Логина и Пароля

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.

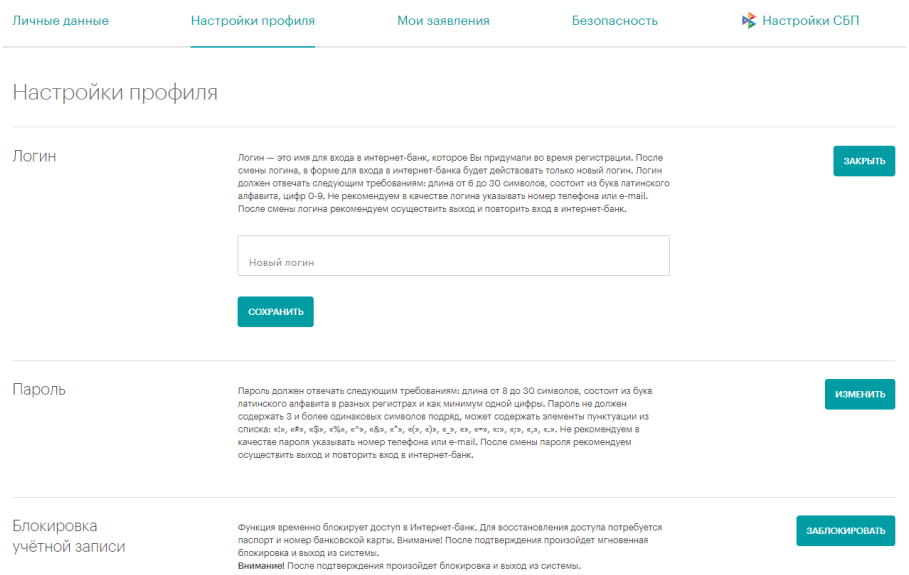
Для смены Транспортного пароля при первом входе в Систему будет открыто соответствующее окно:



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:

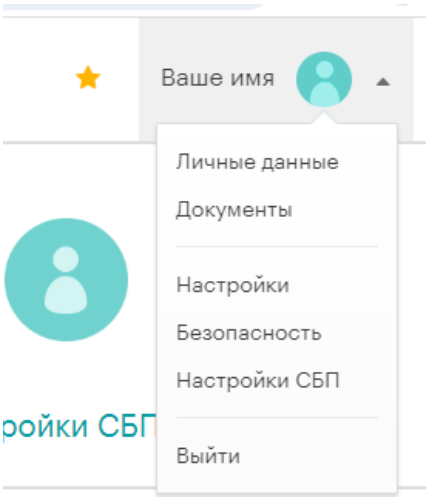


При успешном подтверждении WEB-версии Системы «Интернет-банк» откроется страница «**Настройки профиля**», в которой можно будет изменить Логин. В целях безопасной работы с Системой «Интернет-банк» и защиты финансовых операций настоятельно рекомендуется произвести изменение Логина при первом входе в Систему.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



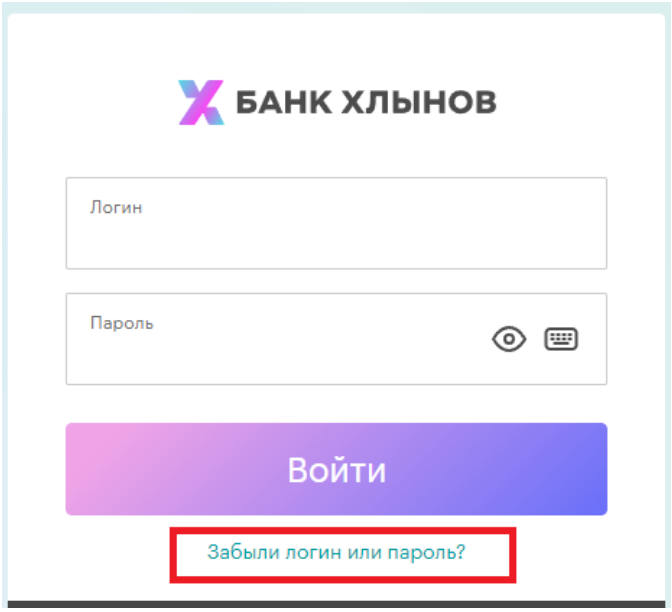
В дальнейшем для входа в Систему необходимо будет использовать Постоянные Логин и Пароль.

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.

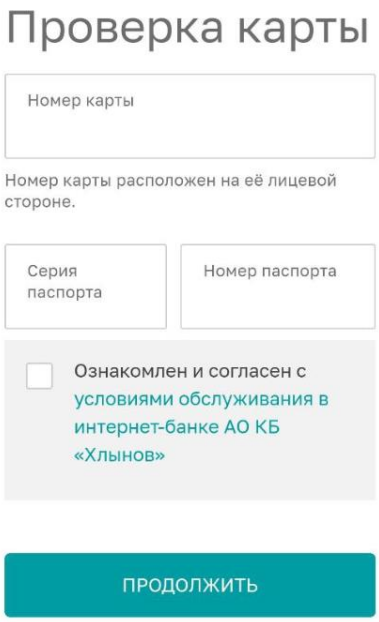


9. Забыли логин или пароль

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?».**

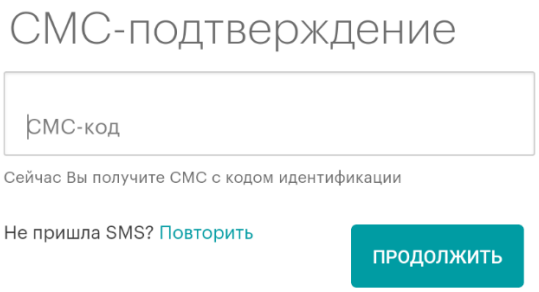


После нажатия кнопки «**Забыли логин или пароль»** система предложит ввести данные Банковской карты и документа, удостоверяющего личность. Для восстановления доступа к Системе необходимо ознакомиться с Условиями обслуживания в интернет-банке АО КБ «Хлынов» и отметить пункт «Ознакомлен и согласен с Условиями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

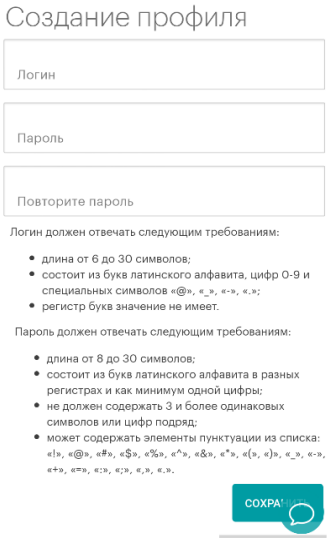


После нажатия кнопки «**Продолжить»** необходимо ввести Разовый код безопасности из SMS-

сообщения.



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



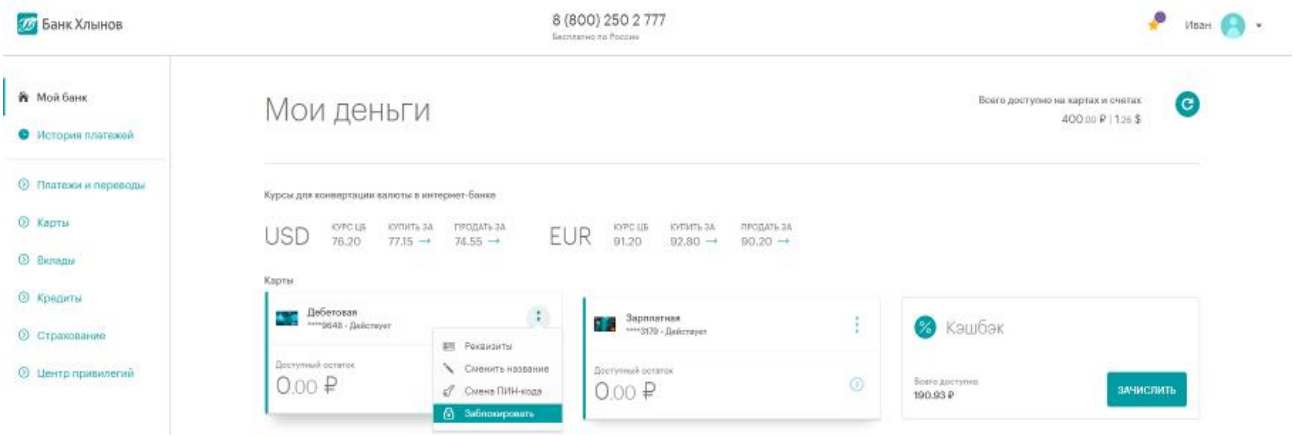
10. Блокировка Карты

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.

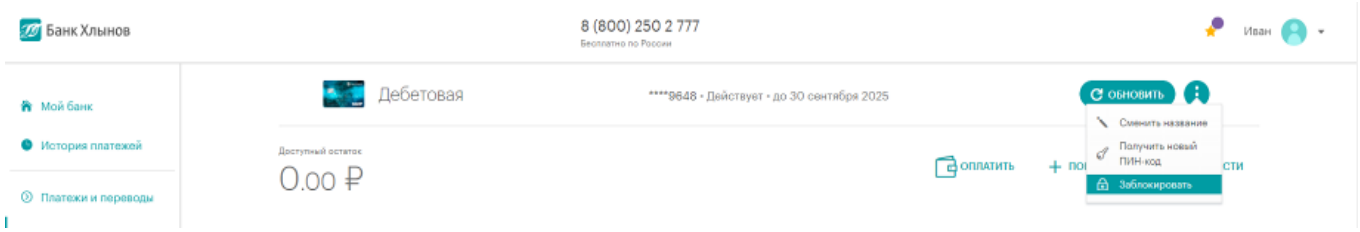
Разблокировка производится в офисе Банка при личном присутствии владельца Карты, наличии оригинала документа, удостоверяющего личность, и письменного заявления на разблокировку Карты или при обращении в Чат после входа в Систему.

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

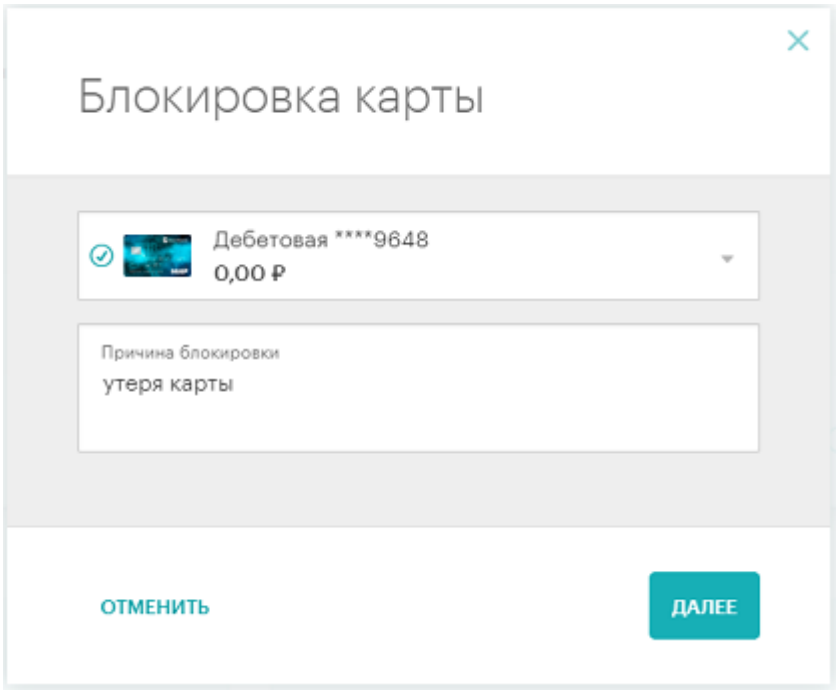
Заблокировать Карту вы можете находясь на главной странице Системы с помощью кнопки «**Заблокировать»** в выпадающем меню:



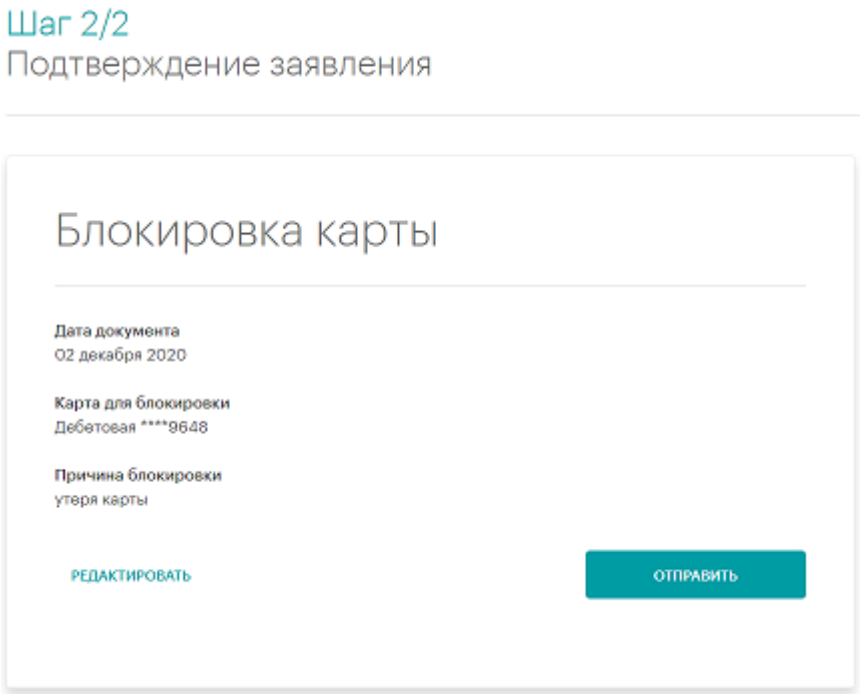
Также возможность заблокировать Карту предоставлена на странице детальной информации по Карте из выпадающего меню:



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.



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».**

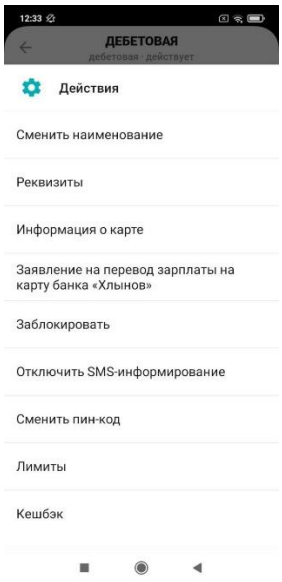


Если Вы передумали отправлять заявку на блокировку Карты, то нажмите кнопку «**Редактировать»,** затем – «**Отменить»**.

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

2) **С использованием Мобильного приложения**

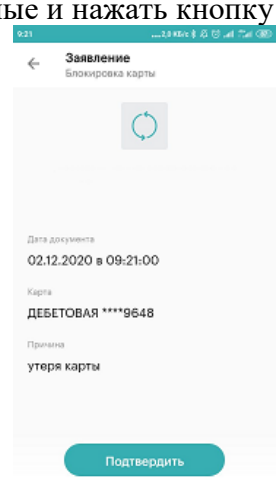
Возможность заблокировать Карту представлена на странице детальной информации по Карте с помощью кнопки «Действия» с иконкой шестеренки. В выпадающем меню необходимо выбрать «**Заблокировать»**:



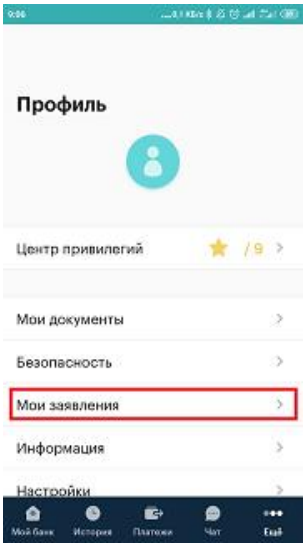
В результате откроется окно блокировки Карты, в котором необходимо указать причину

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».

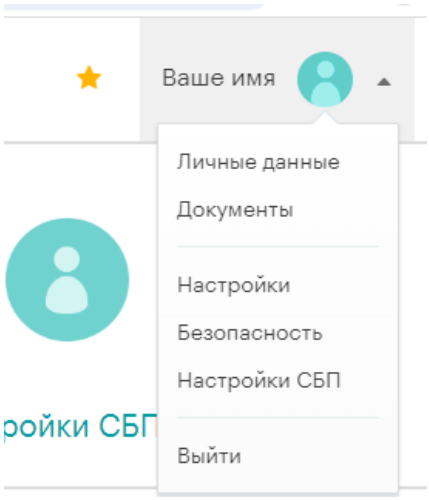


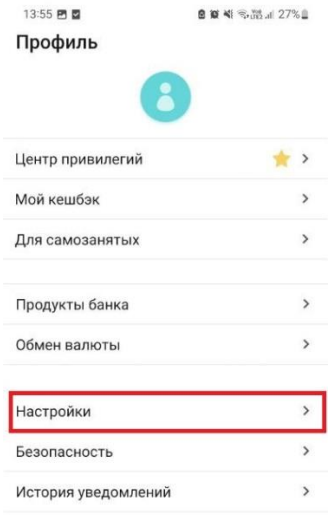
11. Личные данные

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.

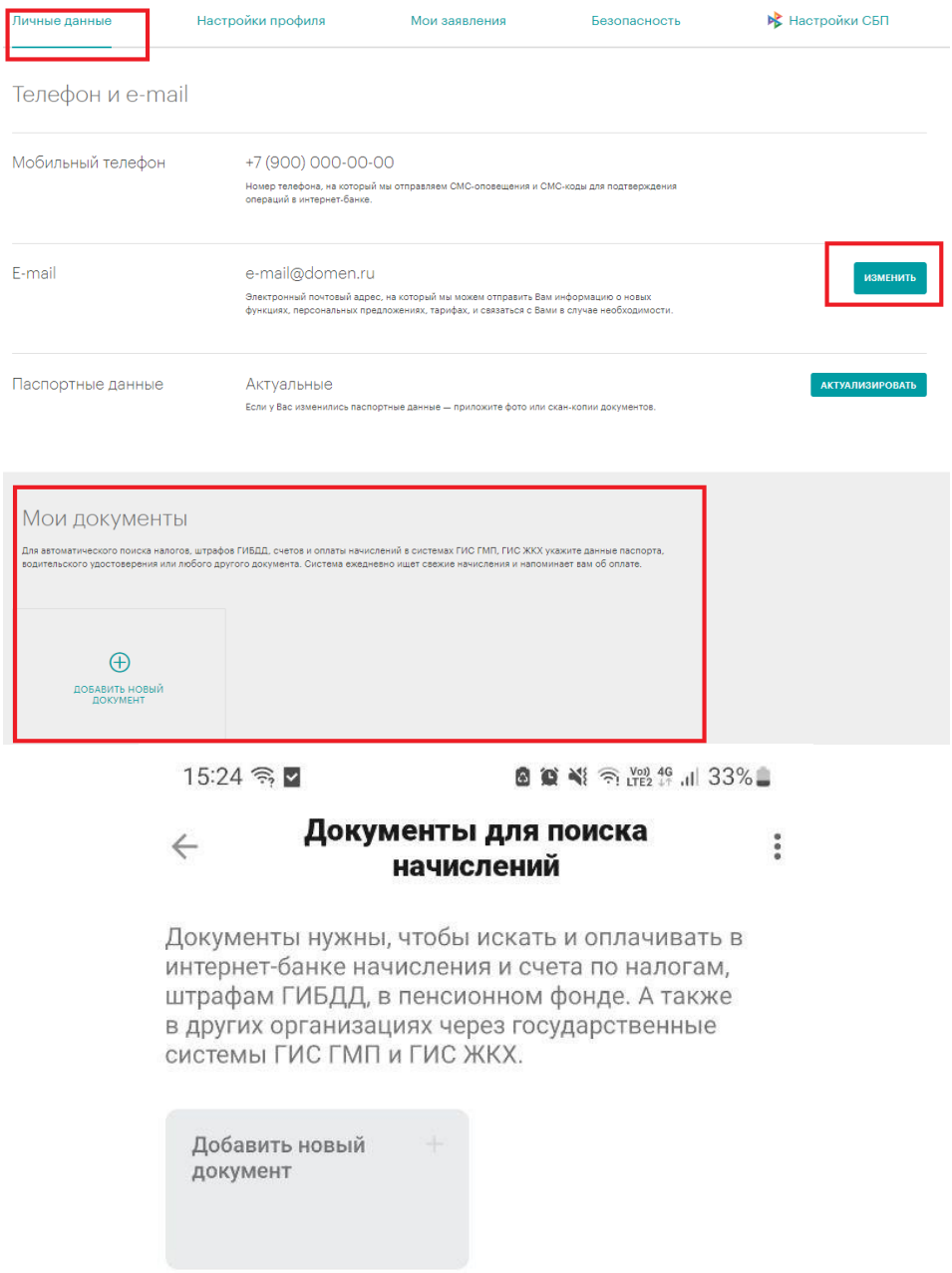
Электронный почтовый адрес необходим для направления Клиенту Банком писем информационного характера, а также связи в случае необходимости. Чтобы добавить электронную почту необходимо нажать «**Добавить**», ввести в открывшемся окне свой адрес электронной почты и нажать на кнопку «**Сохранить**».





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**».

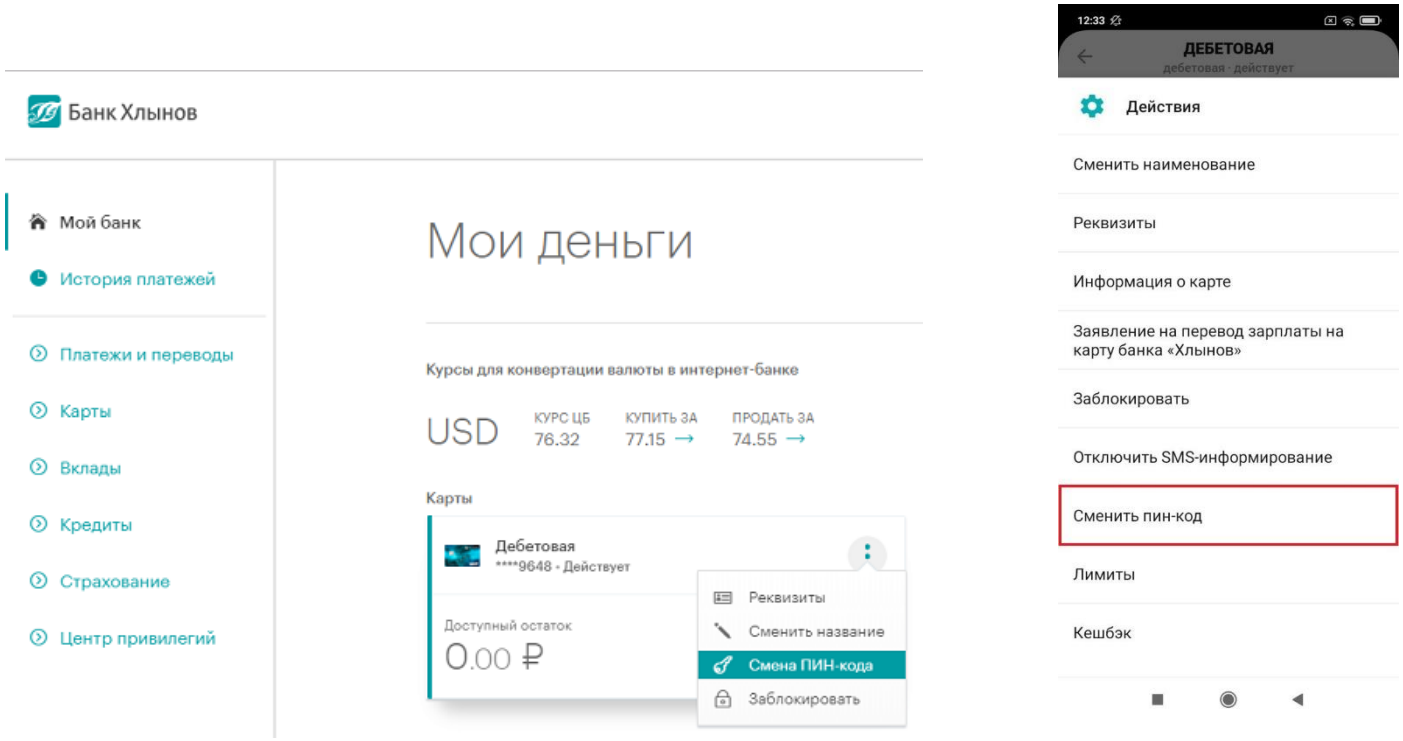


12. Смена ПИН-кода Карты

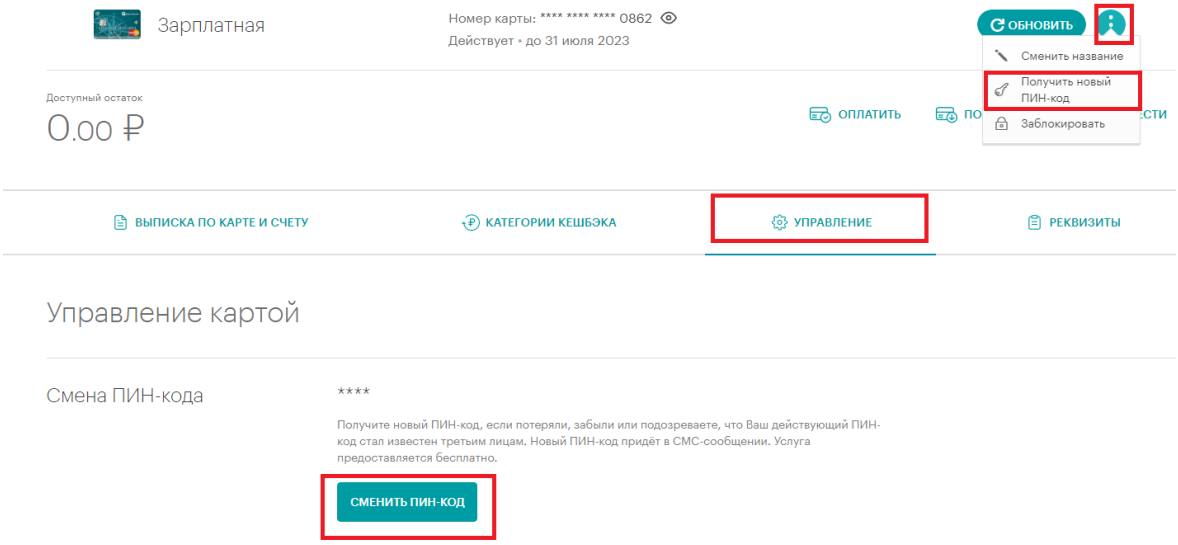
Обратите внимание! В целях безопасности: не сообщайте ПИН-код Карты третьим лицам. Помните, что сотрудники Банка никогда не попросят вас назвать ПИН-код.

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.

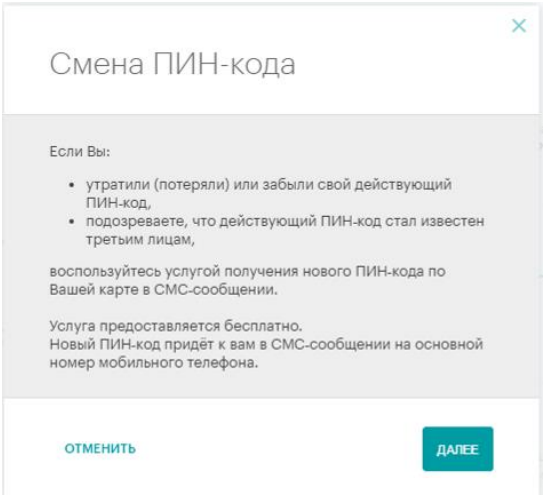
Сменить ПИН-код возможно с главной страницы Системы с помощью кнопки «**Смена ПИН-кода»** в выпадающем меню Карты (в WEB-версии Системы «Интернет-банк») или через кнопку «Действия» в Карте (через мобильное приложение):



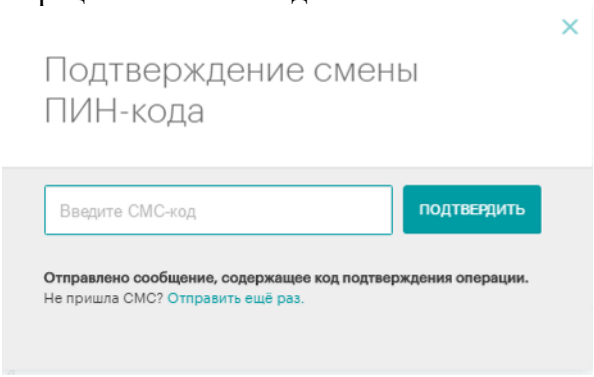
Также в WEB-версии смена ПИН-кода возможна со страницы детальной информации по карте из выпадающего меню ⋮ или во вкладке «**Управление»** с помощью кнопки «**СМЕНИТЬ ПИН-КОД**»:



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.



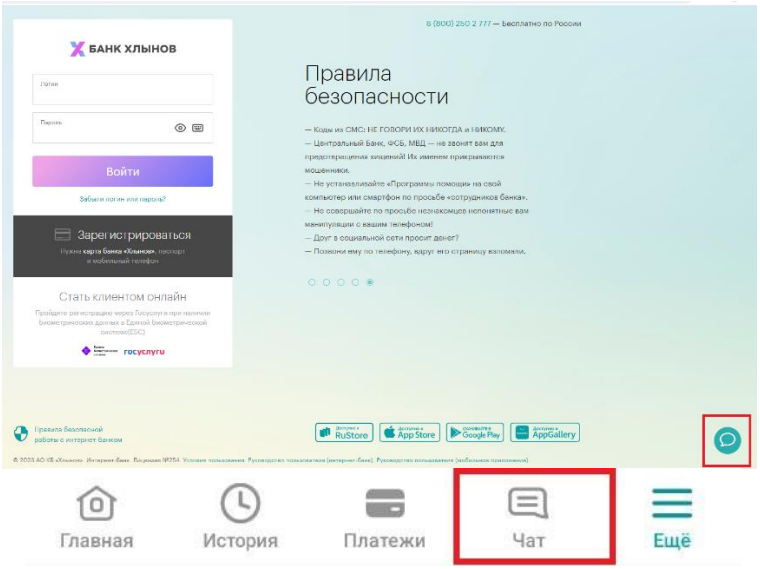
Основные правила обеспечения безопасности ваших средств на Карте:

- 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.

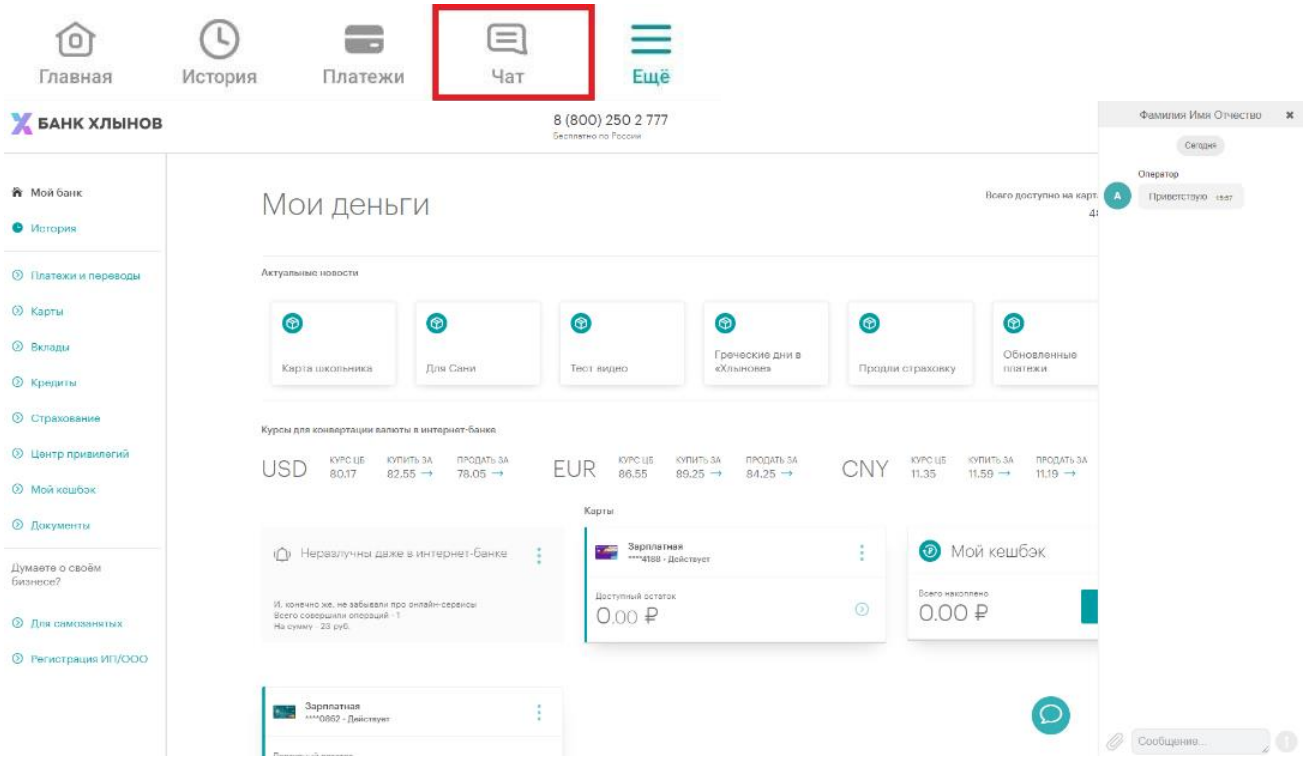
13. Чат

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.



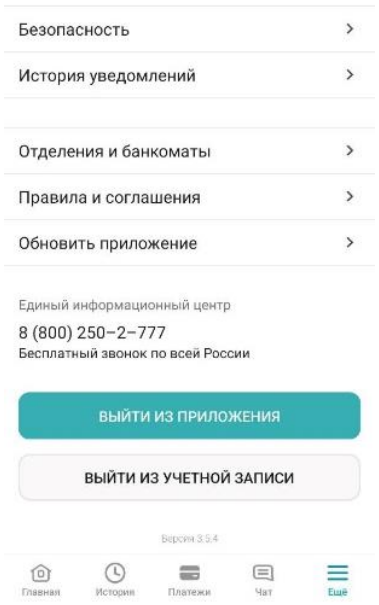
Клиент, авторизованный в Системе (совершил вход в Систему с использованием Логина и Пароля или короткого Пин-кода при использовании Мобильного приложения), имеет возможность вести персонализированную электронную переписку с Банком. В этом случае Банк может направлять на исполнение заявления от Клиента 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 лиц[1].

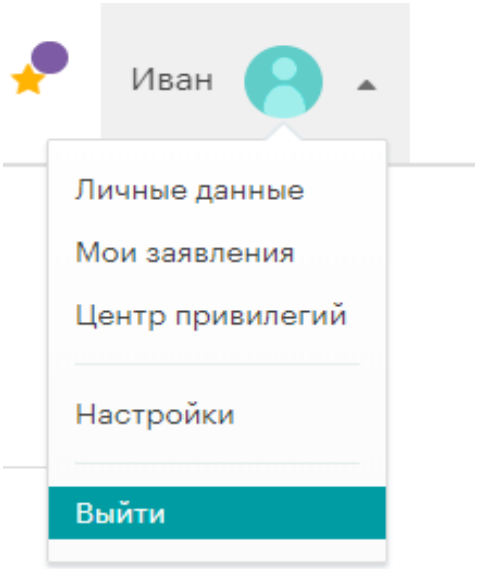


[1] Часть 2 статьи 5 и часть 2 статьи 6 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

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 недостоверных 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;

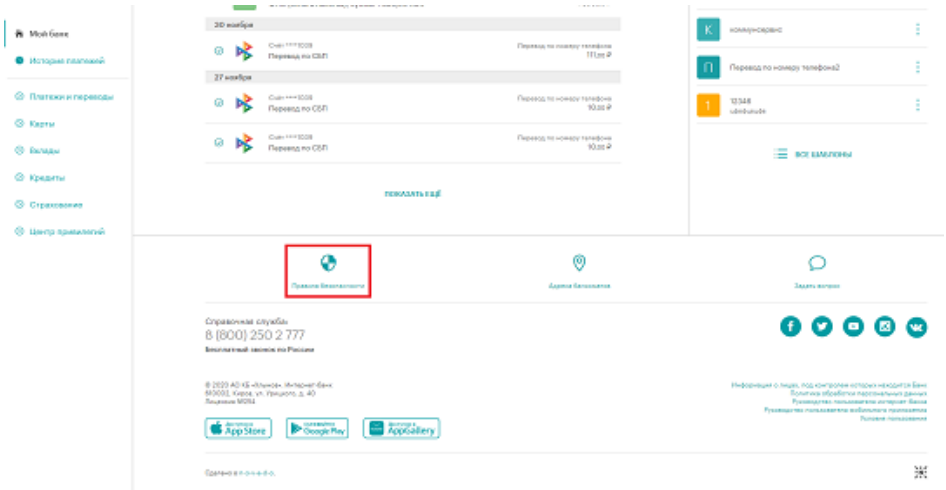
– **своевременно устанавливайте обновления** программного обеспечения своих устройств, рекомендуемые компанией-производителем;

– 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 недостоверных 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 утрате 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;

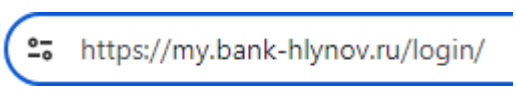
Если у вас есть подозрения что кто-либо использует ваш Логин и Пароль или совершаются операции, которых вы не совершали, необходимо обратиться в Банк по телефону 8 (800) 250-2-777 (звонок по России бесплатный). Помните, что при работе со своими счетами в Системе «Интернет-банк» следует быть такими же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

16. Проверка подлинности сайта

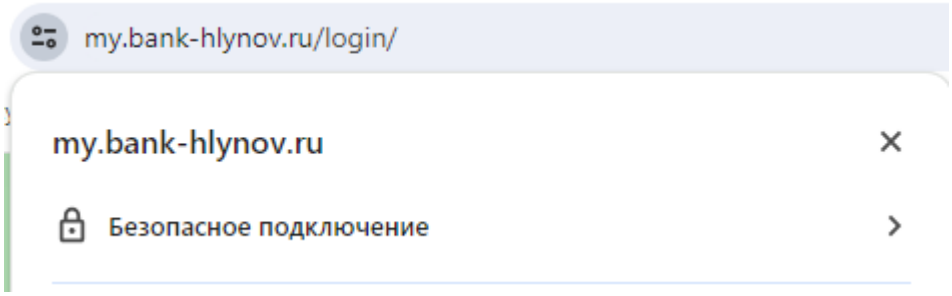
Для надежной работы в Системе рекомендуется использовать современные Интернет-браузеры, например, Chrome, Яндекс браузер.

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

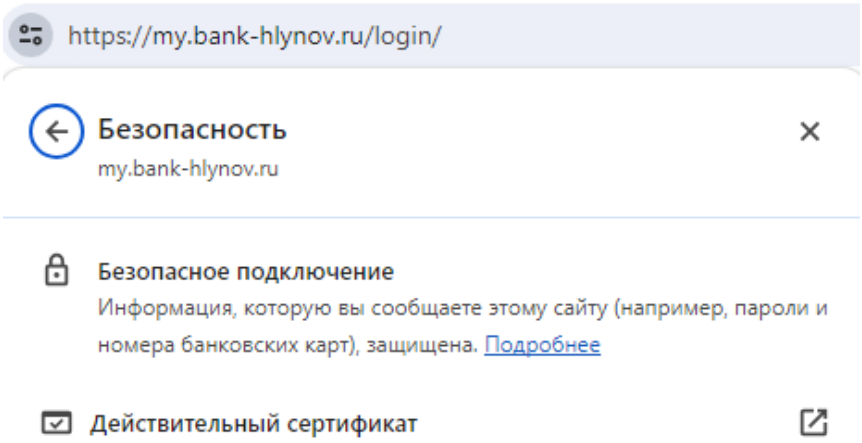
1. Проверьте адрес в адресной строке браузера: https://my.bank-hlynov.ru/



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

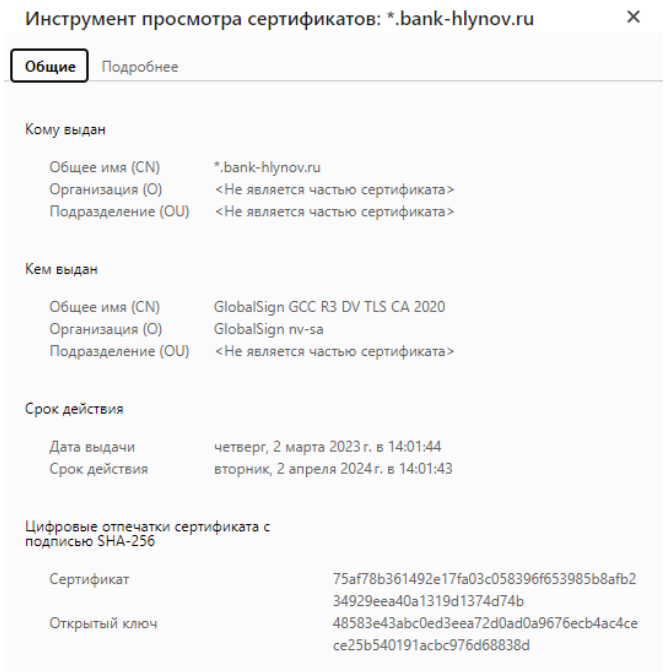


3. В открывшемся списке выберите пункт «**Безопасное подключение**», затем «**Действительный сертификат**»:



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.

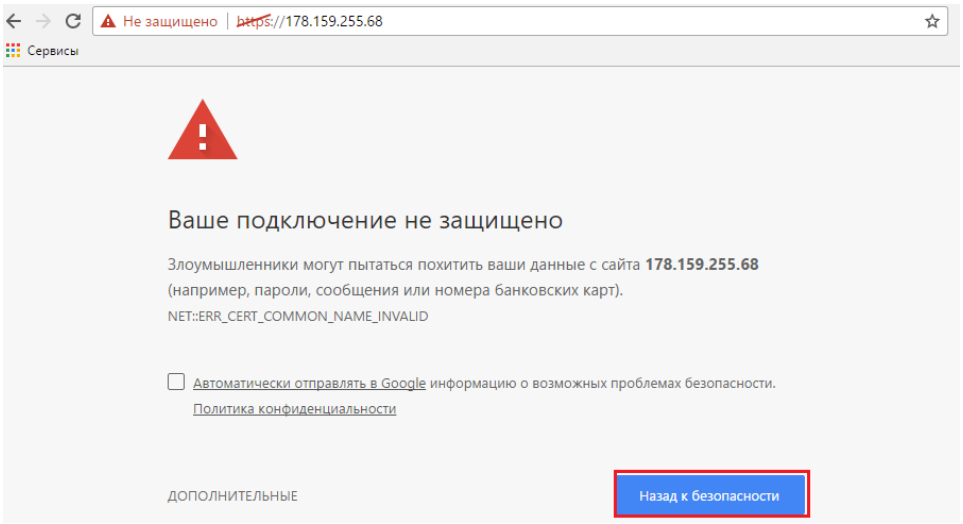
Кем выдан показывается название центра сертификации, ответственного за выдачу сертификата. К наиболее доверенным ЦС относятся Comodo, Symantec, Thawte, GeoTrust, GlobalSign, AlphaSSL и RapidSSL, и некоммерческий Let`s Encrypt. Желательно не доверять сайтам с сертификатами от малоизвестных сертификационных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

Срок действия показывает период действия SSL сертификата.

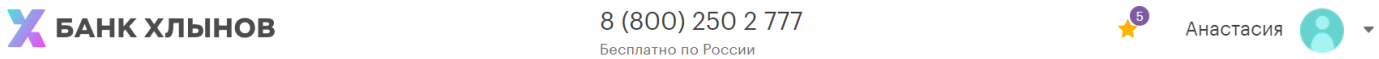
Далее можно закрыть окно с информацией о сертификате.

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.



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).**