



УРАЛПРОМБАНК

УТВЕРЖДЕНО
Протоколом Правления
№ 55 от 27.08.2025
АО «УРАЛПРОМБАНК»

Правила использования электронного средства платежа - системы «Интернет-Банк»

применяются с «01» сентября 2025 года

«Уральский Промышленный Банк» (акционерное общество) (АО «УРАЛПРОМБАНК»), зарегистрированное в Центральном банке РФ 11.07.1994, регистрационный № 2964, место нахождения: Россия, 454090, город Челябинск, улица Свободы, дом 97 (местонахождение постоянно действующего исполнительного органа Банка), к/с 30101810600000000906 в Отделении Челябинск, БИК 047501906, ИНН 7449014065, КПП 745301001, ОГРН 1027400001727, телефон: (351) 239-65-65, 239-65-55, официальный сайт в сети «Интернет»: www.uralprombank.ru, лицензия ЦБ РФ на осуществление банковских операций № 2964 (далее – Банк).

Оглавление:

1. Общие положения
2. Условия использования Системы
3. Порядок осуществления переводов денежных средств с использованием Системы
4. Порядок использования Системы
5. Порядок проверки электронной подписи в Системе
6. Размер вознаграждения Банка, порядок его взимания
7. Порядок приостановления и прекращения использования Системы
8. Порядок и способы направления информации, связанной с использованием Системы
9. Порядок предъявления и рассмотрения споров (претензий), связанных с использованием Системы
10. Ответственность сторон
11. Правила безопасного использования Системы, ограничение способов и мест использования Системы, случаи повышенного риска использования Системы
12. Правила защиты конфиденциальной информации в сети Интернет.
13. Аппаратные требования и требования к программному обеспечению, установленному на персональном компьютере Клиента.

1. Общие положения.

Правила использования электронного средства платежа - системы «Интернет-Банк»
применяются с «01» сентября 2025 года

1.1. Настоящие правила определяют порядок, условия предоставления и использования электронного средства платежа - системы «Интернет-Банк» (далее – Система, ИБ), являются обязательными для всех Клиентов Банка – физических лиц (далее – Клиент), заключивших с Банком Договор банковского счета и использующих Систему в целях осуществления переводов денежных средств по счету, открытому в Банке. Настоящие правила размещаются на официальном сайте Банка в сети интернет: www.uralprombank.ru и на информационных стендах, находящихся в офисах Банка.

1.2. Банк вправе в одностороннем порядке изменить настоящие правила с предварительным уведомлением об этом Клиента не позднее пятнадцати календарных дней до даты вступления изменений в силу, путем публикации на официальном сайте Банка в сети интернет: www.uralprombank.ru и на информационных стендах, находящихся в офисах Банка.

В случае несогласия с изменениями или дополнениями, внесёнными в настоящие правила, Клиент имеет право до вступления в силу таких изменений или дополнений в одностороннем порядке отказаться от использования Системы уведомив об этом Банк в порядке, установленном пунктом 8.1 настоящих правил. В случае неполучения Банком до вступления в силу изменённых или дополненных правил, письменного уведомления от Клиента об отказе от использования Системы и если Клиент продолжает использовать Систему, в целях осуществления переводов денежных средств по счету, открытому в Банке, Банк считает это выражением согласия Клиента с изменением настоящих правил.

1.3. Настоящие Правила распространяются на всех Клиентов Банка – физических лиц, заключивших с Банком договор банковского счета, в том числе до вступления в силу настоящих Правил, и использующих Систему в целях осуществления переводов денежных средств по счету, открытому в Банке, от которых Банком не были получены уведомления об отказе от использования Системы, до вступления в силу настоящих правил. Если после вступления в силу настоящих правил Клиент продолжает пользоваться счетом, открытым в Банке, и совершать по нему операции с использованием Системы Банк признает это конклюдентными действиями по присоединению к настоящим правилам в соответствии со статьями 428, 438 Гражданского кодекса Российской Федерации.

1.4. Заключив с Банком договора банковского счета в части использования Системы Клиент признает, что шифровальные (криптографические) средства, используемые для создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи, создания ключа проверки электронной подписи в Системе и обеспечивающие контроль целостности электронной подписи и электронного распоряжения достаточны для подтверждения подлинности и авторства электронного документа.

1.5. В настоящих правилах используются основные понятия, установленные Федеральным законом от 27.06.2011 N 161-ФЗ "О национальной платежной системе", Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи".

2. Условия использования Системы.

2.1 Система является электронным средством платежа, позволяющие Клиенту составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, а также иных технических устройств.

2.2. Использование Системы осуществляется на основании договора банковского счета, заключенного между Банком и Клиентом. После заключения с Банком договора банковского счета Клиент предоставляет в Банк заявление о предоставлении ему доступа к Системе. Подписав указанное заявление Клиент, в соответствии со статьи 428 Гражданского кодекса Российской Федерации присоединяется к настоящим правилам, полностью принимает их условия и обязуется неукоснительно их соблюдать.

2.3. Порядок предоставления электронных средств платежа и осуществления операций с электронными средствами платежа устанавливается нормативным актом Банка России.

2.4. Банк вправе без объяснения причин отказать Клиенту в заключении договора банковского счета в части использования Системы.

2.5. До заключения с Клиентом договора банковского счета в части использования Системы Банк проинформировал Клиента об условиях использования Системы, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования Системы. Данная информация изложена в настоящих правилах. Подписанием заявления о предоставлении доступа к Системе Клиент подтверждает, что ознакомлен с указанной информацией.

2.6. Банк обязан незамедлительно информировать Клиента о совершении каждой операции с использованием Системы путем направления Клиенту соответствующего уведомления в порядке, установленном пунктом 8.2 настоящих правил, но не позднее одного рабочего дня, следующего за днем совершения операции.

2.7. Банк обязан обеспечить возможность направления ему Клиентом уведомления об утрате Системы и (или) о ее использовании без добровольного согласия Клиента.

2.8. Банк обязан фиксировать направленные Клиенту и полученные от Клиента уведомления, а также хранить соответствующую информацию не менее трех лет.

2.9. Банк обязан предоставлять Клиенту документы и информацию, которые связаны с использованием клиентом Системы, в порядке, установленном пунктом 8.2. настоящих правил по запросу Клиента.

2.10. Клиент вправе в любое время отказаться от использования Системы уведомив об этом Банк в порядке, установленном пунктом 8.1 настоящих правил.

2.11. Заключив с Банком договор банковского счета в части использования Системы Клиент признает, что документ, в том числе электронное распоряжение, переданное с использованием Системы, подписанное электронной подписью Клиента, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью Клиента.

2.12. Банк обязан отказать Клиенту в заключении договора банковского счета в части использования Системы в случае, если Банком от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа. Банк обязан незамедлительно уведомить Клиента об отказе в

заключении договора банковского счета в части использования Системы с указанием причины такого отказа."

3. Порядок осуществления переводов денежных средств с использованием Системы.

3.1. Переводы денежных средств осуществляются Банком на основании договора банковского счета, заключенного между Банком и Клиентом, в соответствии с Правилами осуществления переводов денежных средств в АО «УРАЛПРОМБАНК», размещенными на официальном сайте Банка в сети интернет: www.uralprombank.ru и на информационных стендах, находящихся в офисах Банка.

3.2. Переводы денежных средств с использованием Системы осуществляются на основании электронного распоряжения, подписанного электронной подписью Клиента в пользу получателей денежных средств. Электронные распоряжения передаются, принимаются к исполнению, исполняются и хранятся в электронном виде в Системе.

3.3. Перевод денежных средств осуществляется за счет денежных средств Клиента, находящихся на его банковском счете. Осуществление переводов денежных средств с использованием Системы возможно по всем счетам Клиента, открытым в Банке, а также по тем, которые будут открыты Клиентом в Банке в будущем (в соответствии с режимом работы счета).

3.4. Банк осуществляет круглосуточный прием электронных распоряжений Клиента, передаваемых в Системе. Банк принимает распоряжение Клиента к исполнению и направляет Клиенту электронное уведомление в Системе о приеме распоряжения к исполнению с указанием информации, позволяющей Клиенту идентифицировать распоряжение и дату приема его к исполнению. Электронные уведомления в Системе направляются Клиенту незамедлительно.

3.5. Банк обязан при приеме к исполнению электронного распоряжения Клиента удостовериться в праве Клиента распоряжаться денежными средствами, проверить реквизиты перевода, достаточность денежных средств для исполнения распоряжения Клиента, а также выполнить иные процедуры приема к исполнению распоряжений Клиентов, предусмотренные законодательством Российской Федерации.

3.6. Банк не принимает электронные распоряжения Клиента к исполнению, если право Клиента распоряжаться денежными средствами не удостоверено и (или) если реквизиты перевода не соответствуют установленным требованиям. Об отказе в приеме электронного распоряжения Банк незамедлительно направляет Клиенту электронное уведомление в Системе.

3.7. В целях противодействия осуществлению переводов денежных средств без согласия Клиента Банк, на основании заявления Клиента устанавливает в отношении операций, осуществляемых с использованием Системы, ограничения на осуществление операций Клиентом либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции Клиента, так и в разрезе видов операций.

4. Порядок использования Системы.

4.1. Система представляет собой технологически обособленный ресурс в сети интернет, находящийся в распоряжении Банка, являющийся его интеллектуальной собственностью, размещенный по адресу: <https://pay.uralprombank.ru>.

4.2. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и настоящими правилами в Системе используется **простая электронная подпись**, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом (Клиентом).

4.3. При входе Клиента в Систему, Банк производит аутентификацию Клиента, посредством логина и пароля, содержащих необходимые комбинации символов, введенных Клиентом в соответствующую форму. Логин и пароль сообщаются Банком Клиенту в ПИН-конверте, выдаваемом Клиенту, при получении банковской Карты.

«Аутентификация» – удостоверение права использования Клиентом электронного средства платежа — системы «Интернет-Банк», осуществляемое Банком посредством проверки логина и пароля Клиента, содержащих комбинации символов, введенных им в соответствующую форму при входе в систему «Интернет-Банк». Аутентификация в «Мобильном банке» может быть осуществлена на основании биометрической верификации пользователя платформ iOS и/или Android.

4.4. Переводы денежных средств с использованием Системы осуществляются на основании электронных распоряжений, подписанных электронной подписью Клиента посредством введения цифрового кода, содержащегося в разовом ключе электронной подписи.

4.5. Разовые ключи электронной подписи сообщаются Банком Клиенту посредством средства подтверждения. Клиентам доступны следующие средства подтверждения:

- 1) таблица разовых ключей;
- 2) программа «UPBkeyGen» для мобильных платформ;
- 3) генератор одноразовых паролей eTokenPASS;
- 4) системные средства биометрической верификации платформ iOS и Android, при использовании приложения «Мобильный банк»;
- 5) постоянный PIN при использовании приложения «Мобильный банк»;
- 6) push-уведомления.

4.6. Карточка с таблицей разовых ключей передается Клиенту Банком при личном обращении Клиента в Банк, при предъявлении документа, удостоверяющего личность Клиента. Разовые ключи электронной подписи в таблице покрыты защитным слоем, делающим невозможным доступ третьих лиц и работников Банка к информации о значениях разовых ключей электронной подписи. При использовании ключа электронной подписи защитный слой стирается, значение ключа становится доступным Клиенту.

4.7. В распоряжении Клиента может находиться одновременно несколько карточек с таблицей разовых ключей, из которых в данный момент действующей является только одна. В действующей таблице разовых ключей один и только один разовый ключ электронной подписи является текущим в данный момент времени.

4.8. При запросе подтверждения значения ключа в Системе Банк сообщает Клиенту порядковый номер текущего разового ключа электронной подписи в находящейся в распоряжении

Клиента действующей таблицы разовых ключей и проверяет правильность разового ключа электронной подписи, сообщенного Клиентом. Положительный результат проверки правильности разового ключа электронной подписи, сообщенного Клиентом, является электронной подписью Клиента и подтверждением электронного распоряжения.

4.9. Таблица разовых ключей считается действующей с момента первого использования Клиентом любого разового ключа из таблицы разовых ключей и до использования всех разовых ключей данной таблицы разовых ключей либо подачи Клиентом в Банк заявления об отмене действия таблицы разовых ключей.

4.10. Клиент может прекратить использование действующей таблицы разовых ключей, находящейся в его распоряжении, путем подачи в Банк письменного заявления об отмене действия таблицы разовых ключей.

4.11. Клиент вправе установить на свой мобильный телефон программу генерации ключей (паролей) «UPBkeyGen» либо приобрести в отделениях Банка генератор одноразовых паролей «eTokenPASS». Установка программы «UPBkeyGen» для мобильных устройств с операционными системами iOS и Android осуществляется из официальных магазинов приложений производителей данных операционных систем.

4.12. Банк предоставляет подробную инструкцию по установке и использованию указанного приложения, либо приобретенного в Банке по выбору Клиента генератора одноразовых паролей «eTokenPASS» в целях успешной генерации паролей и их использования Клиентом самостоятельно.

4.13. Банк оставляет за собой право без предупреждения Клиентов вносить изменения в приложение «UPBkeyGen», публиковать альтернативные релизы приложения в магазинах приложений Apple и (или) Google, либо снимать приложение с публикации в данных магазинах.

4.14. Установка приложения «UPBkeyGen» способом, несоответствующим указанным выше (не только, но и в частности из неофициальных магазинов приложений, путем прямой передачи по беспроводным интерфейсам (Bluetooth, Wi-Fi и т.п.) с одного устройства на другое) будет признана Банком противоречащей условиям настоящих правил. Банк оставляет за собой право запретить использование установленного данным способом приложения «UPBkeyGen» в качестве средства подтверждения в Системе.

4.15. Клиент вправе в любой момент использовать те средства подтверждения, которые он самостоятельно выбрал и (или) подключил в настройках Системы.

4.16. Модель контроля доступа, реализуемая в Системе, основана на использовании маркера доступа (IDtoken). При использовании приложения «Мобильный банк» Клиент вправе выбрать в настройках Системы и использовать в последующем в качестве средства подтверждения системные средства биометрической верификации платформ iOS и (или) Android. При подаче Клиентом электронного распоряжения в Банк положительный результат проверки правильности IDtoken при одновременном успешном прохождении биометрической верификации платформ iOS и (или) Android, является электронной подписью Клиента и подтверждением электронного распоряжения. Банк для данных электронных распоряжений признает в качестве ключа электронной подписи Клиента IDtoken.

4.17. **«Мобильный банк»** — приложение для мобильных телефонов, обеспечивающее доступ к ИБ посредством мобильной (беспроводной) связи. «Мобильный банк» не является электронным средством платежа (далее – ЭСП). «Мобильный банк» является альтернативным способом с собственным графическим интерфейсом пользователя, позволяющим Клиенту

воспользоваться ИБ. Порядок Аутентификации Клиента в «Мобильном банке» идентичен Аутентификации в ИБ.

При использовании приложения «Мобильный банк» и установлении в настройках Системы в качестве средства подтверждения системных средств биометрической верификации платформ iOS и (или) Android, Клиент обязан установить постоянный PIN. Данный постоянный PIN при использовании Клиентом приложения «Мобильный банк» может использоваться в качестве средства подтверждения и быть запрошен:

- при неуспешном прохождении биометрической верификации платформ iOS и/или Android;
- как самостоятельное средство подтверждения.

Постоянный PIN, как Средство подтверждения, признается Банком в качестве ключа электронной подписи Клиента.

4.18. Клиент вправе выбрать в настройках Системы для приложения «Мобильный банк» и использовать в последующем в качестве средства подтверждения push-уведомления. Значение push-уведомления при положительном результате проверки Банком его правильности признается Банком в качестве ключа электронной подписи Клиента.

4.19. Банк может самостоятельно определять вид электронного распоряжения и/или максимальную сумму электронного распоряжения, для которых у Клиента не будет запрашиваться разовый пароль. Если иное не установлено настоящими правилами без ввода разового пароля могут быть исполнены следующие электронные распоряжения:

1) вход в Систему и «Мобильный банк» (по умолчанию для новых Клиентов). Для Клиентов, у которых в настройках Системы установлено требование ввода разового ключа, его запрос при входе в Систему сохраняется;

2) перевод между своими счетами Клиента, открытыми в Банке;

3) конвертация валют между счетами Клиента, открытыми в Банке;

4) управление холдами (произвольное блокирование средств на счете Клиента);

5) электронное распоряжение из раздела госплатежи;

6) настройки сервиса быстрых платежей платежной системы Банка России;

7) оплата мобильной связи до 500,00 руб. в день на всех российских операторов связи, сверх 500,00 руб. в день - запрос разового ключа;

8) настройки Системы

Для данных электронных распоряжений (действий) признает в качестве ключа электронной подписи Клиента IDtoken.

4.20. Использование кодового слова.

4.20.1. Кодовое слово устанавливается Клиентом и сообщается Банку при заключении договора банковского счета после обязательной идентификации Клиента.

4.20.2. Использование Клиентом кодового слова осуществляется:

- в случае личного обращения в офис Банка - в устной форме;
- в случае доступа через Центр поддержки клиентов - по телефону в устной форме;

4.20.3. В случае необходимости замены кодового слова, в том числе при его утрате, Клиент может обратиться с заявлением о замене в офис Банка. Замена кодового слова производится при условии обязательной идентификации Клиента.

4.20.3. Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения невозможности доступа третьих лиц к информации о Кодовом слове, находящейся в распоряжении Банка.

4.21. Использование шаблонов электронных распоряжений в Системе.

4.21.1. Для составления электронного распоряжения в Системе Клиент вправе использовать соответствующий данной операции шаблон электронного распоряжения. Шаблоны подразделяются на две категории:

- шаблоны общего пользования, доступные для использования всеми Клиентами, содержащие реквизиты переводов, часто используемых Клиентами Банка (оплату услуг мобильных операторов, налоги, штрафы и др.) и
- персональные шаблоны, созданные для определенного Клиента, содержащие реквизиты перевода, используемые только данным Клиентом.

4.21.2. Каждый шаблон электронного распоряжения общего пользования характеризуется набором реквизитов, включающим постоянные, хранящиеся в шаблоне, реквизиты, и переменные реквизиты, которые Клиент заполняет самостоятельно. Персональные шаблоны создаются Клиентом самостоятельно и сохраняются в Системе.

4.21.3. Шаблоны общего пользования создаются Банком в одностороннем порядке и могут быть изменены или отменены без согласования с Клиентом. Об изменении или отмене шаблонов общего пользования Банк извещает Клиента в Системе.

4.21.4. Создавая или изменяя персональный шаблон электронного распоряжения, Клиент поручает Банку произвести перевод денежных средств по реквизитам, указанным в шаблоне электронного распоряжения, и самостоятельно несет ответственность за их правильность.

4.21.5. Банк вправе самостоятельно устанавливать в шаблонах Системы различные лимиты на суммы переводов денежных средств по счету (в рублях Российской Федерации либо в эквивалентной сумме в иностранной валюте по курсу Банка России на день проведения перевода денежных средств). В случае установления лимита информация доводится до Клиента в виде сообщения в шаблоне Системы.

4.21.6. Банк вправе отказать в оформлении персонального шаблона или запретить использование ранее оформленного персонального шаблона, если предусмотренные шаблоном операции противоречат законодательству Российской Федерации, нормативным актам Банка России или настоящим правилам. Отмена Банком использования персонального шаблона влечет прекращение использования основанных на нем длительных поручений на перевод денежных средств. Клиент оповещается о запрещении использования ранее оформленного персонального шаблона.

4.22. Компрометация Системы - утрата Банком или Клиентом уверенности в том, что ИБ не может быть использован третьими лицами, в том числе в случае разглашения третьим лицам логина и пароля, необходимых для входа в ИБ.

4.23. Компрометация средств подтверждения – утрата, хищение, несанкционированное копирование, передача средств подтверждения, находящихся у Клиента. Любые другие виды разглашения содержания ключа ЭП Клиента, а также случаи, когда нельзя достоверно установить,

что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

5. Порядок проверки электронной подписи.

5.1. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

- 1) простая электронная подпись содержится в самом электронном документе;
- 2) ключ простой электронной подписи применяется в соответствии с настоящими правилами и в созданном и (или) отправленном электронном документе содержится информация, указывающая на Клиента, от имени которого был создан и (или) отправлен электронный документ.

5.2. При получении электронного распоряжения, составленного в Системе, Банк удостоверяется в праве Клиента распоряжаться денежными средствами посредством проверки электронной подписи Клиента, присоединённой к электронному распоряжению. Положительный результат проверки правильности разового ключа электронной подписи, введенного Клиентом, является электронной подписью Клиента и подтверждением электронного распоряжения.

5.3. При запросе подтверждения значения ключа в Системе Клиент вводит значение разового ключа электронной подписи полученного с использованием выбранного Клиентом средства подтверждения, Банк проверяет правильность разового ключа, сообщенного Клиентом. Положительный результат проверки правильности разового Ключа, сообщенного Клиентом, является электронной подписью Клиента и подтверждением электронного распоряжения.

5.4. Средство подтверждения считается действительным в момент его использования, если одновременно выполнены следующие условия:

- между Банком и Клиентом заключен Договор банковского счета;
- Клиент самостоятельно выбрал и (или) подключил средство подтверждения в настройках Системы;
- срок действия средства подтверждения не истек;
- средство подтверждения не было отменено Клиентом или Банком;
- Клиент прошел аутентификацию посредством логина и пароля при входе в Систему.

6. Размер вознаграждения Банка, порядок его взимания

6.1. За предоставление доступа к Системе (установку) и использование Системы Клиент уплачивает Банку вознаграждение (комиссию) в порядке и размере, установленном Тарифами Банка, действующими на момент оказания услуги.

6.2. Банк вправе в одностороннем порядке изменить размер вознаграждения за предоставление доступа к Системе (установку) и использование Системы, указанный в Тарифах Банка, с предварительным уведомлением об этом Клиента не позднее пятнадцати календарных

дней до даты вступления изменений в силу, путем публикации на официальном сайте Банка в сети интернет: www.uralprombank.ru и на информационных стендах, находящихся в офисах Банка.

6.3. В случае несогласия с изменениями, внесёнными в Тарифы Банка, Клиент имеет право до вступления в силу таких изменений в одностороннем порядке отказаться от использования Системы. В случае неполучения Банком до вступления в силу изменённых Тарифов письменного уведомления от Клиента об отказе от использования Системы, Банк считает это выражением согласия Клиента с изменением Тарифов Банка.

6.4. Плата за услуги Банка, предусмотренные настоящими правилами, взимается Банком из денежных средств Клиента, находящихся на его счете, если иное не предусмотрено договором банковского счета, путем выставления расчетных документов, оплачиваемых без дополнительных распоряжений Клиента в порядке, предусмотренном действующим законодательством Российской Федерации, нормативными актами Банка России, договором банковского счета, Тарифами Банка. Согласие Клиента на осуществление указанных операций считается предоставленным Банку при заключении Договора банковского счета. О списании денежных средств со счета Банк направляет Клиенту уведомление не позднее дня, следующего за днем списания в порядке, установленном пунктом 8.2. настоящих правил.

6.5. В случае недостаточности на счете Клиента денежных средств, необходимых для оплаты соответствующих услуг Банка, Банк имеет право отказать Клиенту в предоставлении указанных услуг.

7. Порядок приостановления и прекращения использования Системы.

7.1. Использование Клиентом Системы может быть приостановлено или прекращено Банком на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования Системы в соответствии с настоящими правилами, а также в случаях, предусмотренных Федеральным законом от 27.06.2011 N 161-ФЗ "О национальной платежной системе" и в иных случаях, предусмотренных законодательством РФ.

7.2. При приостановлении или прекращении использования Клиентом Системы в случаях, предусмотренных настоящими правилами, Банк обязан в день такого приостановления или прекращения, предоставить Клиенту информацию о приостановлении или прекращении использования Системы с указанием причины такого приостановления или прекращения, в порядке, установленном пунктом 8.2 настоящих правил.

7.3. Приостановление или прекращение использования Клиентом Системы не прекращает обязательств Клиента и Банка, возникших до момента приостановления или прекращения указанного использования.

7.4. Использование Клиентом Системы может быть приостановлено или прекращено Банком при производстве технических работ на аппаратно-программном обеспечении Системы, в случае обнаружения угроз из сети интернет, направленных на нарушение целостности аппаратно-программного обеспечения Системы, а также в случае возникновения обстоятельств непреодолимой силы, не зависящих от воли сторон.

7.5. В случае, если Банк получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, и если отсутствуют сведения федерального органа исполнительной власти в

сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии с [частью 8 статьи 27](#) Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе", Банк в рамках реализуемой им системы управления рисками и в порядке, предусмотренном настоящими правилами, вправе приостановить использование Клиентом Системы на период нахождения сведений, относящихся к Клиенту и (или) его электронному средству платежа, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента. В случае, если использование Клиентом Системы не было приостановлено в соответствии с настоящим пунктом, в период нахождения сведений, относящихся к Клиенту и (или) его электронному средству платежа, в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента Банк может осуществлять переводы денежных средств с использованием Системы по распоряжению Клиента в пользу получателей - физических лиц на сумму не более 100 тысяч рублей в месяц.

7.6. Банк обязан приостановить использование Клиентом Системы, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, при наличии сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемых в соответствии с [частью 8 статьи 27](#) Федерального закона от 27.06.2011 N 161-ФЗ "О национальной платежной системе", на период нахождения указанных сведений в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

7.7. После приостановления использования Клиентом Системы в случаях, предусмотренных пунктами 7.5. и 7.6. настоящих правил, Банк обязан в порядке, предусмотренном пунктом 8.2. настоящих правил, незамедлительно уведомить Клиента о приостановлении использования Системы, а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении сведений, относящихся к Клиенту и (или) его электронному средству платежа, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

7.8. В случае наличия у Банка оснований полагать, что включение сведений, относящихся к Клиенту и (или) его электронному средству платежа, в базу данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента является необоснованным, Банк вправе самостоятельно (без участия Клиента) направить в Банк России мотивированное заявление об исключении сведений, относящихся к Клиенту и (или) его электронному средству платежа, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.

7.9. В случае получения в порядке, установленном Банком России, информации об исключении сведений, относящихся к Клиенту и (или) его электронному средству платежа, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента Банк обязан незамедлительно возобновить использование Клиентом Системы и незамедлительно уведомить Клиента о возможности использования Системы при отсутствии иных оснований для приостановления использования Системы в соответствии с законодательством Российской Федерации или настоящими правилами.

7.10. При приостановлении использования Системы в соответствии с пунктом 7.6. настоящих правил, использование Клиентом Системы может быть возобновлено Банком до исключения сведений, относящихся к Клиенту и (или) его электронному средству платежа, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, по заявлению Клиента в случае наличия у Банка оснований полагать, что сведения относящиеся к Клиенту и (или его) электронному средству платежа включены в базу данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, необоснованно.

8. Порядок и способы направления информации, связанной с использованием Системы.

8.1. Уведомления или иные сообщения, направляемые Клиентом в адрес Банка, должны быть направлены заказным почтовым отправлением с уведомлением о вручении по адресу: Россия, 454090, город Челябинск, улица Свободы, дом 97 (местонахождение постоянно действующего исполнительного органа Банка) или вручаются Клиентом представителю Банка лично. При этом датой получения отправления считается дата, указанная работником почтовой службы в уведомлении о вручении или дата, указанная на копии письма при вручении.

8.2. Уведомления или иные сообщения направляемые Банком в адрес Клиента, в том числе в случаях, когда действующим законодательством или настоящими правилами предусмотрена обязанность Банка направить Клиенту уведомление, информировать Клиента, предоставить Клиенту какую-либо информацию, должны быть:

- направлены электронным сообщением по адресу электронной почты, сообщенному Клиентом Банку в заявлении на открытие банковского счета или ином заявлении Клиента, определяющем порядок направления сообщений Клиенту;

- путем размещения необходимой информации на официальном сайте Банка www.uralprombank.ru, в разделе «личный кабинет». Вход в «личный кабинет» осуществляется по логину и паролю, указанным в ПИН-конверте, выданном Клиенту при получении Банковской карты к счету.

С момента направления электронного сообщения указанным способом либо с момента размещения необходимой информации на официальном сайте Банка www.uralprombank.ru, в разделе «личный кабинет» обязанность Банка, предусмотренная настоящим пунктом, считается исполненной надлежащим образом. При этом датой получения сообщения Клиентом будет считаться дата направления/размещения Банком электронного сообщения.

8.3. Дополнительно уведомления или иные сообщения, указанные в пункте 8.2. настоящего договора, могут быть предоставлены Банком Клиенту при личном обращении Клиента по адресу Банка: Россия, 454090, город Челябинск, улица Свободы, дом 97 (местонахождение постоянно действующего исполнительного органа Банка).

8.4. Уведомления или иные сообщения, направляемые Клиентом в адрес Банка или Банком в адрес Клиента, дополнительно могут быть направлены в электронной форме посредством Системы.

8.5. Уведомления или иные сообщения, указанные в пункте 8.2. настоящих правил, иная информация, дополнительно могут направляться Банком Клиенту иным способом, указанным в заявлении Клиента на открытие банковского счета или в ином заявлении Клиента, определяющем

порядок направления сообщений Клиенту.

Размер платы за услуги Банка по направлению дополнительных сообщений (уведомлений, информации) Клиенту определяется Тарифами Банка, действующими на момент предоставления услуги.

8.6. В случае утраты электронного средства платежа – Системы и (или) ее использования без добровольного согласия Клиента, а равно компрометации Системы и/или компрометации средства подтверждения, Клиент обязан незамедлительно направить соответствующее уведомление Банку, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции.

Соответствующее уведомление может быть сделано Клиентом в режиме круглосуточного доступ по следующим контактным телефонам Банка: (351) 239-65-65, (351) 239-65-55, 8-800-775-05-55 (звонок по России бесплатный) или по адресу электронной почты Банка: post@uralprombank.ru.

При этом Клиент должен сообщить свои Ф.И.О., слово пароль, а также ответить на ряд вопросов, установленных технологическим порядком Банка. Устное сообщение должно быть подтверждено письменным заявлением Клиента в срок не позднее следующего рабочего дня, направленным в порядке, установленном пунктом 8.1 настоящих правил. Фактом, подтверждающим принятие Банком сообщения Клиента, является номер принятого сообщения, зарегистрированный сотрудником Банка для Клиента.

8.7. Банк обязан незамедлительно приостановить операции по счету Клиента с использованием Системы при получении соответствующего уведомления Клиента, указанного в пункте 8.6. настоящих правил.

8.8. При получении от Клиента уведомления, указанного в пункте 8.6. настоящих правил, после осуществления списания денежных средств с банковского счета Клиента Банк, обязан незамедлительно направить оператору по переводу денежных средств, обслуживающему получателя средств, уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств по **форме** и в **порядке**, которые установлены нормативным актом Банка России.

9. Порядок предъявления и рассмотрения споров (претензий), связанных с использованием Системы.

9.1. При возникновении споров, конфликтных ситуаций, связанных с использованием Системы, сторона, заявляющая разногласие (инициатор спора) обязана направить другой стороне заявление (претензию), с подробным изложением обстоятельств спора, реквизитов электронного распоряжения, при исполнении которого возник спор, в порядке, установленном пунктами 8.1, 8.2 настоящих правил.

9.2. Банк обязан рассматривать заявления Клиента, в том числе при возникновении споров, связанные с использованием Клиентом Системы, а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более тридцати дней со дня получения таких заявлений, а также не более шестидесяти дней со дня получения заявлений в случае использования Системы для осуществления трансграничного перевода денежных средств.

9.3. До разрешения спора Банк приостанавливает использование Системы.

9.4. Спор, связанный с использованием Системы, не урегулированный в претензионном порядке, может быть передан на разрешение суда по истечении срока указанного в пункте 9.2. настоящих правил в порядке, установленном действующим законодательством Российской Федерации. В случаях, установленных Федеральным законом от 04.06.2018 N 123-ФЗ "Об уполномоченном по правам потребителей финансовых услуг" потребитель финансовых услуг вправе заявлять в судебном порядке требования к Банку, только после получения от финансового уполномоченного решения по обращению.

10. Ответственность сторон

10.1. Банк не несет ответственности в случаях приостановления или прекращения использования Системы, указанных в настоящих правилах, а также по обстоятельствам, не зависящим от Банка, в том числе в случае сбоя программного обеспечения или оборудования, не принадлежащих Банку.

10.2. Банк не несет ответственности за убытки, возникшие у Клиента при нарушении Клиентом настоящих правил.

10.3. Право использования Системы является исключительным и непередаваемым. В случае передачи Клиентом ключа электронной подписи, пароля, логина и (или) кода, необходимых для использования Системы третьим лицам, Клиент в полном объеме несет ответственность за действия, совершенные такими третьими лицами с использованием Системы, а также за ущерб, причиненный такими третьими лицами Банку и Клиенту.

10.4. Банк не несёт ответственность за ущерб, причинённый Клиенту в результате использования третьими лицами электронной подписи Клиента.

10.5. Банк не несет ответственность за правомерность и правильность надлежащим образом оформленного Клиентом электронного распоряжения, а также за убытки, понесенные Клиентом вследствие отказов и несвоевременных действий лиц, в пользу которых осуществляется перевод денежных средств по поручению Клиента.

10.6. Банк не несет ответственность за последствия исполнения распоряжений, подписанных электронной подписью Клиента, выданных неуполномоченными лицами, в том числе и в тех случаях, когда Банк не смог установить факт выдачи электронного распоряжения неуполномоченными лицами, в том числе лицами, осуществляющими мошеннические действия.

10.7. Банк не несет ответственность за некорректную работу Системы на оборудовании Клиента с установленным на нем нелицензионным программным обеспечением.

10.8. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из сторон, прямо или косвенно запрещающих указанные в настоящих правилах виды деятельности или препятствующие выполнению сторонами настоящих правил, если сторона, пострадавшая от их влияния, доведет до сведения другой стороны известие о случившемся не позднее следующего дня после возникновения этих обстоятельств в порядке, установленном пунктами 8.1, 8.2. настоящих правил.

11. Правила безопасного использования Системы, ограничение способов и мест использования Системы, случаи повышенного риска использования Системы

11.1. Использование Системы потенциально несет в себе риски неблагоприятных последствий, для ее пользователя, в том числе связанных с хищением денежных средств, которые могут возникнуть в случае несанкционированного доступа третьих лиц к Системе.

11.2. В Системе используются современные механизмы обеспечения безопасности и позволяющие удобно пользоваться услугой, обеспечивая при этом высокий уровень ее надежности и безопасности. Эффективность данных механизмов зависит от выполнения Клиентом следующих правил:

1) Контролируйте доступ к Вашим средствам подтверждения.

2) При установке нового пароля (логина) для доступа к Системе не используйте простые комбинации. Лучше всего, если пароль (логин) будет длинной не менее восьми символов, состоять из заглавных и строчных букв, а также цифр. Это обеспечит защиту от взлома пароля.

3) Запомните логин и пароль для доступа в Систему. Никогда не записывайте их в местах, легкодоступных посторонним лицам (на стикерах, на мониторе, в файлах на рабочем месте и т.д.).

4) Никому никогда не передавайте средства подтверждения.

5) Помните, что сотрудники Банка никогда и ни в какой форме не будут запрашивать Ваш пароль (логин). Игнорируйте любые сообщения по электронной почте, запрашивающие Ваши пароли либо данные счетов или содержащие ссылку на Web-страницу, где Вам предлагается эти данные ввести. Сообщайте в Банк обо всех подобных фактах.

6) Используйте современное антивирусное программное обеспечение. Регулярно обновляйте антивирусные базы и проводите полную антивирусную проверку Вашего компьютера и (или) мобильного телефона, планшетного компьютера для своевременного обнаружения вредоносных программ.

7) Установите и используйте персональный брандмауэр (firewall) на вашем компьютере. Это позволит предотвратить несанкционированный доступ к информации на компьютере.

8) Устанавливайте самые последние обновления Вашего браузера и операционной системы.

9) Регулярно проверяйте электронный почтовый ящик Клиента Банка - Bank-mail. Дополнительно подключите SMS- или E-mail-уведомление о движении средств по счету.

10) Не сообщайте третьим лицам, кодовое слово, логин, пароль и ключи средств подтверждения, используемые в Системе.

11) Перед установкой программы «Мобильный банк» или «UPBkeyGen» убедитесь, что:

- скачиваете программу из официального магазина приложений для данного устройства (операционной системы);
- наименование приложения полностью соответствует следующему написанию «URALPROMBANK» или «UPBkeyGen», а наименование вендора приложения соответствует следующему наименованию: АО «УРАЛПРОМБАНК», JSCUralsIndustrialBank. Избегайте установку приложений, копирующих символику АО «УРАЛПРОМБАНК», но имеющих иные наименования, в том числе иное наименование вендора (разработчика) данного

приложения.

12) Для мобильных устройств на операционных системах iOS и Android запрещено использование приложений «Мобильный банк», «UPBkeyGen» и (или) осуществление доступа в Систему посредством интернет-обозревателя в случае присутствия скомпрометированной среды, установленной на мобильном устройстве:

- для операционной системы Android – получение прав администратора (root-права) и (или) установка альтернативных графических интерфейсов пользователя («прошивок») сторонних разработчиков, и не входящих в пакет обновлений, распространяемых официальным вендором операционной системы и (или) производителем мобильного устройства;
- для операционной системы iOS – джейлбрейк (Jailbreak).

13) Ежедневно проверяйте расходные и приходные операции в Системе. Сохраняйте в секрете пароль, логин и ключи средств подтверждения, необходимые для использования Системы. Принимайте все меры по предотвращению несанкционированного использования Системы.

14) Не осуществляйте посредством Системы незаконные финансовые операции, незаконную торговлю и любые другие операции в нарушение законодательства Российской Федерации.

15) При любых подозрениях на компрометацию кодового слова, логина, пароля, ключей средств подтверждения, а также при возникновении любых необычных ситуаций при работе с Системой – немедленно обратитесь в Банк: Контактные телефоны АО «УРАЛПРОМБАНК», работающие круглосуточно: (351) 239-65-65, (351) 239-65-55, 8-800-775-05-55 (звонок по России бесплатный), адрес электронной почты: post@uralprombank.ru.

12. Правила защиты конфиденциальной информации в сети Интернет.

Следование данным правилам позволит Вам обезопасить себя и свои денежные средства от мошеннических действий на подложных сайтах в сети Интернет. Фишинг (англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо ссылка на страницу приложения для мобильных устройств, копирующего фирменную символику настоящего приложения. Оказавшись на таком сайте, пользователь может сообщить мошенникам ценную информацию, позволяющую получить доступ к аккаунтам и банковским счетам. Аналогично использование подложного приложения для мобильного устройства влечет те же неблагоприятные последствия. Люди, обманутые такими мошенническими приемами, открывают злоумышленникам номера своих банковских карт, пароли и другую конфиденциальную информацию. Чтобы не попасть в такую ситуацию, крайне важно быть уверенным, что все транзакции совершаются в защищенной среде, которую успешно обеспечивает Банк.

Способы защиты:

12.1. Игнорировать письма, запрашивающие Вашу конфиденциальную информацию.

- Банк НИКОГДА не запрашивает какую-либо конфиденциальную информацию по электронной почте.

- Банк никогда не присылает в тексте письма ссылки, которые переадресуют Вас на сайт, где нужно ввести какую-либо конфиденциальную информацию.

12.2. Заходить в Систему путем ввода его URL-адреса через адресную строку браузера, либо через сохраненную ВАМИ в «Избранном» ссылку.

12.3. Проверять регулярно движение по своим счетам. При наличии подозрительной операции по счету, банковской карте немедленно уведомлять об этом Банк.

12.4. Проверять уровень защиты сайтов. При посещении сторонних сайтов (Интернет-магазинов и т.д), где требуется использование Ваших конфиденциальных данных, для начала проверьте его безопасность.

- Проверьте Web-адрес в адресной строке браузера. Адрес должен начинаться с «https://» («s» от security), а не с обычного «http://». Если это так, то данный сайт располагается на защищенном сервере.
- Вы можете проверить уровень криптозащиты, поведя курсором мыши над иконкой в виде «замка» внизу страницы. Если иконка в виде «закрытого замка», то сайт защищен. Кликните по этой иконке, и Вы должны увидеть окно с данными сертификата защиты.

12.5. Обеспечить защиту своего компьютера или мобильного устройства.

- Установите антивирусное программное обеспечение и, обеспечив его обновление, вы получите помощь по обнаружению и деактивации вредоносных программ, а использование антиспам программного обеспечения обезопасит ваши почтовые ящики от получения фишинговых писем.
- Также важно, особенно для пользователей широкополосного доступа к интернету, установить межсетевой экран. Это поможет, блокируя связи с нежелательными источниками, сохранить информацию на вашем персональном компьютере в безопасности.
- Убедитесь, что у вас установлена современная версия Web-браузера, и вы установили для нее самые последние обновления. Если у вас нет этих обновлений, обратитесь на Web-сайт производителя браузера.

12.6. Незамедлительно уведомляйте Банк, если какое-либо подозрительное действие было произведено с Вашими денежными средствами или Вам было прислано подозрительное письмо или предложение от имени Банка.

13. Аппаратные требования и требования к программному обеспечению, установленному на персональном компьютере Клиента.

Для успешного и бесперебойного функционирования Системы персональное устройство вычислительной техники Клиента должно соответствовать:

13.1. Персональный компьютер и программное обеспечение, установленное на нем, должны удовлетворять следующим требованиям:

Требования к аппаратным ресурсам компьютера:

- процессор с тактовой частотой 1ГГц и выше;
- разрешение экрана монитора не менее 1024×768;
- размер шрифта экрана — обычный размер (96 dpi);
- оперативная память (ОЗУ) - не менее 512 MB;

– свободное пространство на жестком диске: ох86 – 850 МБ о х64 – 2 ГБ;

13.2. Требования к программному обеспечению:

1) Для успешного функционирования Системы необходимо, чтобы на компьютере Клиента была установлена одна из следующих операционных систем (ЛИЦЕНЗИОННАЯ):

- Windows не ниже 8.1;
- Windows Server не ниже 2008 R2 SP1;
- Поддерживаемые архитектуры: ох86 ох64.

2) Компоненты, необходимые для работы в Системе:

- InternetExplorer 11,
- Интернет-браузер на ядре Chromium версии 139.0. или более поздней;
- Microsoft .NET 3.5 SP1 или Microsoft .NET.

13.3. Для мобильных устройств на операционных системах iOS и Android запрещено использование приложений «Мобильный банк», «UPBkeyGen» и (или) осуществление доступа в Систему посредством интернет-обозревателя в случае присутствия скомпрометированной среды, установленной на мобильном устройстве:

- Для операционной системы Android – получение прав Администратора (root-права) и (или) установка альтернативных графических интерфейсов пользователя («прошивок») сторонних разработчиков, и не входящих в пакет обновлений, распространяемых официальным вендором операционной системы и (или) производителем мобильного устройства;
- Для операционной системы iOS – джейлбрейк (Jailbreak).