

г. Киров

УТВЕРЖДЕН  
приказом председателя правления АО КБ «Хлынов»  
от 25.06.2018 № 108-ОД

### **Договор об использовании электронного средства платежа система «iBank 2»**

Коммерческий банк «Хлынов» (акционерное общество), именуемый в дальнейшем «Банк», с одной стороны, и Клиент, с другой стороны, при совместном упоминании в дальнейшем именуемые «Стороны», заключили настоящий Договор об использовании электронного средства платежа «Система «iBank 2», именуемый в дальнейшем «Договор», о нижеследующем.

#### **1. Термины, применяемые в Договоре.**

Термины, применяемые в тексте настоящего Договора, используются в следующем значении:

1.1. Электронное средство платежа (ЭСП) – средство и (или) способ, 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, в том числе платежных карт, а также иных технических устройств.

1.2. Система «iBank 2» (система) - совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях с целью осуществления переводов денежных средств. В рамках настоящего Договора система «iBank 2» является электронным средством платежа.

1.3. Электронный документ, ЭД – совокупность байт, содержащая финансовый документ (платежное распоряжение) или информационное сообщение в системе «iBank 2».

1.4. Электронная подпись, ЭП – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1.5. Клиент – юридическое лицо / индивидуальный предприниматель /лицо, занимающееся частной практикой, заключившее(-ий) с Банком настоящий Договор.

- 1.6. Ключ электронной подписи, ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП.
- 1.7. Ключ проверки электронной подписи, ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.
- 1.8. Пара ключей электронной подписи, пара ключей ЭП – ключ ЭП и соответствующий ему ключ проверки ЭП.
- 1.9. Подлинная электронная подпись, подлинная ЭП – ЭП в ЭД, проверка которой с использованием соответствующего ключа проверки ЭП дает положительный результат.
- 1.10. Активная пара ключей электронной подписи, активная пара ключей ЭП – пара ключей ЭП, зарегистрированных Банком в системе «iBank 2», и используемых сотрудником Клиента для работы в системе «iBank 2».
- 1.11. Сертификат ключа проверки электронной подписи, сертификат – документ на бумажном носителе, выданный удостоверяющий центром, заверенный подписью владельца ключа проверки ЭП, подписью руководителя и оттиском печати Клиента.
- 1.12. Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов, а также иные функции, предусмотренные Федеральным законом Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». В рамках настоящего Договора функции удостоверяющего центра выполняются Банком.
- 1.12. Сочетание подписей – комбинации ЭП лиц, наделенных правом подписи, необходимые для подписания ЭД, содержащих распоряжение Клиента (в соответствии соглашением между Банком и Клиентом и/или карточкой с образцами подписей и оттиском печати).
- 1.13. Аппаратное средство усиленной электронной подписи, аппаратное средство усиленной ЭП – специализированное аппаратное средство, предназначенное для генерации пары ключей ЭП, хранения сгенерированных ключей ЭП, формирования ЭП в документах в соответствии с утвержденными стандартами (ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) с использованием встроенного в устройство сертифицированного средства криптографической защиты информации.
- 1.14. Программное средство усиленной электронной подписи, программное средство усиленной ЭП – программный модуль, входящий в состав системы «iBank 2», предназначенный для генерации пары ключей ЭП, формирования ЭП под документами, обеспечивающий защиту информации в соответствии с утвержденными стандартами (ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001) и сертифицированный в соответствии с действующим законодательством.

1.15. Блокировочное слово – уникальное слово, определяемое Клиентом при регистрации в системе «iBank 2» используемое Клиентом для блокирования своей работы в системе «iBank 2» по телефонному звонку в Банк (например, в случае компрометации ключа ЭП).

1.16. Средство подтверждения – электронное или иное средство, используемое для подписи/подтверждения ЭД.

В качестве средства подтверждения могут использоваться, включая, но не ограничиваясь: аппаратное средство усиленной ЭП с ключами ЭП, файловое хранилище ключей ЭП, зарегистрированный в системе мобильный телефон.

1.17. Компрометация средства подтверждения – утрата/хищение средства подтверждения, несанкционированное копирование ключа ЭП, передача ключа ЭП по открытым каналам связи, любые другие признаки осуществления несанкционированных действий в системе «iBank 2», а также случаи, когда нельзя достоверно установить, что произошло со средством подтверждения.

1.18. Одноразовый пароль – динамическая аутентификационная информация, генерируемая для единичного использования.

1.19. Вредоносный код – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и/или Клиента, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

1.20. Многофакторная аутентификация - расширенная аутентификация, метод контроля доступа к компьютеру, в котором для получения доступа к информации необходимо предъявить более одного идентификатора.

1.21. IP-фильтрация - настройка списка IP-адресов, с которых разрешен доступ в систему «iBank 2».

## **2. Предмет Договора**

2.1. Банк оказывает Клиенту услуги по дистанционному распоряжению средствами на счете Клиента с использованием ЭСП, а также по обмену ЭД между сторонами Договора.

2.2. Настоящий Договор является договором присоединения в соответствии со ст.428 ГК РФ. Заключение настоящего Договора между Сторонами осуществляется путем подачи Клиентом в Банк заявления о присоединении Клиента к настоящему Договору по форме Приложения № 2, составленного на бумажном носителе, и принятия заявления Банком.

2.3. Условием предоставления услуг по дистанционному распоряжению средствами на счете Клиента с использованием ЭСП является наличие у Клиента счета в Банке.

2.4. Настоящий Договор распространяется на все счета Клиента.

2.5. Криптографическая защита информации, передаваемой посредством системы «iBank 2», осуществляется Банком на основании действующих лицензий, выданных ФСБ РФ.

### **3. Соглашения сторон**

3.1. Стороны признают, что применяемая в системе «iBank 2» криптографическая защита информации, обеспечивающая шифрование, контроль целостности и создание ЭП с применением программных или аппаратных средств усиленной ЭП достаточна для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД.

3.2. Стороны признают, что применяемая в аппаратных средствах усиленной ЭП технология генерации и хранения ключа ЭП, формирования ЭП под документом с использованием аппаратного средства усиленной ЭП полностью исключает возможность получения прямого доступа к ключу ЭП с целью его копирования, переноса на внешний носитель или использования для формирования ЭП вне устройства.

3.3. Аппаратные средства усиленной ЭП являются собственностью Банка и предоставляются для использования Клиенту на возмездной основе.

3.4. Стороны признают, что при произвольном изменении ЭД, заверенного ЭП, ЭП становится не подлинной, то есть проверка подлинности ЭП дает отрицательный результат.

3.5. Стороны признают, что подделка ЭП сотрудника Клиента, то есть создание Подлинной ЭП в ЭД от имени сотрудника Клиента, невозможна без использования Ключа ЭП сотрудника Клиента.

3.6. Стороны признают, что ЭД с ЭП сотрудников Клиента, полученные Банком по системе «iBank 2», являются доказательным материалом для решения спорных вопросов в соответствии с действующим Положением о процедуре разбора конфликтных ситуаций (Приложение № 4 к настоящему Договору). Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов не являются доказательным материалом.

3.7. Стороны признают, что ключ проверки ЭП считается зарегистрированным в Банке после получения Клиентом сертификата с соответствующими отметками Банка.

3.8. Стороны признают, что ключ проверки ЭП сотрудника Клиента, содержащийся в сертификате, принадлежит соответствующему сотруднику Клиента.

3.9. Стороны признают в качестве единой шкалы времени при работе с системой «iBank 2» московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.10. Стороны признают, что применяемые в системе «iBank 2» механизмы дополнительного подтверждения документов с помощью одноразового пароля, являются надежными.

Документы, требующие подтверждения одноразовым паролем, принимаются Банком к исполнению только в случае надлежащего подтверждения одноразовым паролем, полученным с зарегистрированного по форме Приложения № 3 средства подтверждения Клиента (мобильный телефон).

3.11. Стороны признают, что подделка одноразового пароля, то есть подтверждение ЭД от имени Клиента невозможна без владения соответствующим средством подтверждения.

3.12. Стороны признают, что ЭД должны быть подписаны ЭП лиц, указанных в карточке с образцами подписей и оттиском печати и в сочетании, определенном соответствующим соглашением между Клиентом и Банком.

3.13. Стороны признают, что ЭД, заверенные необходимым количеством ЭП и подтвержденные одноразовым паролем, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке (имеющим необходимые подписи и оттиск печати), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. ЭД без необходимого количества ЭП сотрудников Клиента и/или не подтвержденные одноразовым паролем не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.14. Платежи в пользу бюджета Российской Федерации не требуют подтверждения одноразовым паролем.

3.15. Подтверждение одноразовым паролем ЭД, при совершении платежей в пользу конкретного контрагента Клиента может совершаться единовременно в момент добавления Клиентом такого контрагента в справочник доверенных получателей, хранящийся в системе «iBank 2». В дальнейшем подтверждение ЭД одноразовым паролем при совершении подобных платежей в пользу указанного контрагента Клиента не требуется. Для указанного контрагента правило, указанное в п. 3.13. не применяется. [При использовании одноразовых паролей и списка доверенных получателей]

3.16. Стороны признают, что возможность воспроизведения в электронном виде и на бумажных носителях принятого к исполнению и исполненного платежного распоряжения с отметками Банка осуществляется с использованием системы «iBank 2». Получение платежного распоряжения на бумажном носителе с отметками Банка может осуществляться также в офисе Банка по месту обслуживания счета Клиента в соответствии с графиком работы Банка.

3.17. Перечень электронных документов, передаваемых по системе «iBank 2», приведен в Приложении 5 к Договору.

3.18. Стороны признают надлежащим уведомление Клиента о совершенных операциях с использованием ЭСП хотя бы одним из способов, установленных в Положении о порядке и

способах информирования клиента о совершенных операциях с использованием электронного средства платежа (приложение №6).

#### **4. Права Клиента**

4.1. Клиент имеет право осуществлять эксплуатацию предоставленных Банком сертифицированных ФСБ РФ программных и аппаратных средств усиленной ЭП в системе «iBank 2».

4.2. Клиент имеет право досрочно прекратить действие своей активной пары ключей ЭП и потребовать от Банка заблокировать эту пару ключей ЭП, оформив уведомление по форме Приложения № 8.

4.3. Клиент имеет право по своему усмотрению генерировать новые пары ключей ЭП и регистрировать в Банке новые ключи проверки ЭП.

4.4. Клиент имеет право прекратить регистрацию средства подтверждения, оформив уведомление по форме Приложения № 8.

4.5. Клиент имеет право установить IP-фильтрацию при работе в системе, оформив заявление по форме Приложения № 11.

4.6. Клиент имеет право подключить многофакторную аутентификацию с использованием одноразовых паролей при входе в систему, оформив заявление по форме Приложения № 12.

4.7. Клиент имеет право настроить ограничения на работу в системе по определенному счету, ограничив время приема платежных поручений к исполнению Банком, и/или максимальную сумму платежного поручения, и/или установить перечень возможных получателей платежа, оформив заявление по форме Приложения №15. Факт исполнения заявления Банком фиксируется проставлением в указанном заявлении соответствующей отметки. Для получения информации об исполнении заявления Клиент может обратиться в Банк.

#### **5. Обязанности Клиента**

5.1. Перед началом эксплуатации системы «iBank 2» Клиент обязан получить в Банке и самостоятельно установить на своем рабочем месте [программные модули системы «iBank 2»], программные и аппаратные средства усиленной ЭП.

5.2. На период действия настоящего Договора Клиент обязуется использовать предоставленные средства усиленной ЭП только в системе «iBank 2» без права их продажи или передачи каким-либо способом третьим лицам, обеспечивать возможность контроля со стороны уполномоченных органов за соблюдением требований и условий осуществления деятельности, связанной с использованием криптографических средств.

5.3. Клиент обязан обеспечивать сохранность и целостность программного комплекса системы «iBank 2», включая предоставленные средства усиленной ЭП.

5.4. Клиент обязан обеспечивать информационную безопасность (в том числе защиту от вредоносного кода) рабочих мест ответственных сотрудников, уполномоченных использовать систему «iBank 2» для взаимодействия с Банком. Клиент обязан исключить или максимально ограничить доступ к этим рабочим местам лиц, чья деятельность не связана с осуществлением электронного документооборота с банком.

5.5. Клиент обязан ознакомиться с описанием механизмов защиты системы «iBank 2» и требованиями об обеспечении информационной безопасности своего рабочего места (Приложение №13). В случае если знаний сотрудников Клиента недостаточно для адекватной оценки механизмов защиты системы «iBank 2» и (или) обеспечения информационной безопасности рабочих мест ответственных сотрудников, Клиент вправе обратиться к услугам сторонних специалистов. Оплата услуг специалистов производится Клиентом самостоятельно.

5.6. Клиент обязан в случае прекращения использования системы «iBank 2» уничтожить полученные в Банке программные средства усиленной ЭП.

5.7. Клиент обязан заполнять ЭД в системе «iBank 2» в соответствии с действующим Положением Банка России от 19 июня 2012 г. № 383-П «О правилах осуществления перевода денежных средств» или аналогичным документом, утвержденным вместо указанного Положения.

5.8. Клиент обязан хранить в секрете пароль к Ключу ЭП и не передавать третьим лицам средство подтверждения, используемое в системе «iBank 2», а также обеспечить защиту ключа ЭП и средства подтверждения от несанкционированного использования третьими лицами.

5.9. Клиент обязан обеспечивать использование ключей ЭП только их владельцами (ответственными сотрудниками) в соответствии с установленными правами подписи.

5.10. Клиент обязан по требованию Банка прекратить использование указанного Банком ключа ЭП, сгенерировать новую пару ключей ЭП и зарегистрировать новый ключ проверки ЭП в Банке.

5.11. Клиент обязан предоставить Банку достоверную информацию для связи и информирования о совершенных операциях.

5.12. В случае изменения информации для связи Клиент обязан своевременно предоставить Банку обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом.

5.13. В случае компрометации средства подтверждения Клиент обязан проинформировать Банк в соответствии с Положением о порядке действий сторон в случае компрометации средства подтверждения, указанном в Приложении № 7.

5.14. Клиент обязан исполнять обязательства, возникшие до момента приостановления или прекращения использования Клиентом ЭСП.

5.15. Клиент обязан перед подключением к системе, а также по запросу Банка подтверждать выполнение требований по защите от вредоносного кода (Приложение № 13) с указанием конкретных средств защиты от вредоносного кода и проведенных мероприятий.

5.16. Клиент обязан уведомить Банк о прекращении/изменении полномочий лиц, имеющих действующие сертификаты ключа ЭП, в возможно короткий срок, [но не позднее 5 (Пяти) рабочих дней] с даты прекращения/изменения полномочий. В случае невыполнения указанной обязанности Клиент несет полную ответственность за неблагоприятные последствия, связанные с получением информации по счетам Клиента, а также созданием и подписью ЭД такими лицами после прекращения/изменения их полномочий.

## **6. Права банка**

6.1. Банк имеет право по своему усмотрению без уведомления Клиента блокировать активную пару ключей ЭП Клиента и потребовать от Клиента смены пары ключей ЭП.

6.2. Срок действия криптографического ключа при его изготовлении и хранении на специализированном носителе (usb-токен) устанавливается в 2 (два) календарных года или до наступления события его отзыва или компрометации ключа, в зависимости от того, что наступит ранее.

6.3. Срок действия криптографического ключа при его изготовлении и хранении на незащищенном носителе, при отсутствии в соответствии с договором с Клиентом у лица, получающего ключ, прав на осуществление переводов денежных средств, устанавливается в 1 (один) календарный год или до наступления события его отзыва или компрометации ключа, в зависимости от того, что наступит ранее.

6.4. Срок действия криптографического ключа при его изготовлении и хранении на незащищенном носителе, в случае если Клиенту, получающему ключ, предоставлены права для перевода денежных средств, устанавливается в 1 (один) календарный год при обязательном использовании Клиентом СМС-кодов подтверждения для работы с указанным криптографическим ключом. Факт использования СМС-подтверждения устанавливается по наличию зарегистрированного номера телефона для получения СМС-подтверждений в системе «iBank 2» для лица, получающего сертификат проверки ключа электронной подписи.

6.5. В случае отказа клиента от смс-подтверждения платежей, Банк имеет право заблокировать ключи ЭП на незащищенных носителях.



6.6. Банк регистрирует сертификат проверки ключа электронной подписи в течение 3 (трех) рабочих дней с момента поступления его в Банк.

6.7. При наличии обоснованных подозрений о нарушении Клиентом порядка использования ЭСП, Банк имеет право не производить исполнение полученных от Клиента ЭД, заблокировать использование ЭСП и требовать от Клиента предоставления оформленных в установленном порядке платежных документов на бумажном носителе. Банк обязан незамедлительно, но не позднее 24 (Двадцати четырех) часов, любым способом сообщить Клиенту о возникновении подобных подозрений и необходимости представить платежные документы на бумажном носителе.

6.8 При нарушении Клиентом обязанности по предоставлению Банку достоверной информации для связи с клиентом или обновленной информации в случае ее изменения, Банк вправе приостановить использование клиентом ЭСП до получения от Клиента достоверной информации. При этом Банк прекращает обработку всех ЭД, полученных от Клиента.

6.9. Банк имеет право не возмещать Клиенту сумму операции, совершенной без согласия Клиента при условиях:

- Банк исполнил обязанность по информированию Клиента о совершенной операции и/или
- Клиент не направил Банку уведомление об утрате ЭСП или его использовании без согласия Клиента.

6.10. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию Клиентом ЭСП, Банк имеет право в одностороннем порядке приостановить до момента устранения неисправности использование ЭСП Клиентом. Все документы в этом случае должны передаваться сторонами на бумажных носителях в общем порядке.

6.11. При непогашении Клиентом задолженности, в том числе за ежемесячное обслуживание, Банк вправе по своему усмотрению:

- ограничить перечень услуг, предоставляемых системой;
- приостановить действие настоящего Договора;
- расторгнуть настоящий Договор.

6.12. При отсутствии у Клиента действующих ключей, Банк вправе по своему усмотрению приостановить действие договора до момента оформления ключей и/или расторгнуть настоящий договор в порядке, установленном разделом 13 настоящего договора.

6.13. Банк имеет право после предварительного уведомления Клиента приостанавливать услуги/возобновлять их действие в части использования системы «iBank 2» при несоблюдении Клиентом условий настоящего Договора, а также в рамках исполнения

рекомендаций/требований Банка России, норм действующего законодательства Российской Федерации, в том числе, в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма.

Уведомление в форме электронного сообщения по системе «iBank2» направляется Банком Клиенту в срок не позднее 24 (Двадцати четырех) часов до момента приостановления использования системы с указанием документов/информации, которые необходимо представить в Банк.

## **7. Обязанности банка**

7.1. Банк обязан принимать к исполнению ЭД, полученные по системе «iBank 2» от Клиента, подписанные необходимым количеством ЭП сотрудников Клиента, соответствующие требованиям настоящего Договора и действующему законодательству РФ.

7.2. Банк обязан информировать Клиента о совершенных операциях с использованием электронного средства платежа одним из способов, установленных в Положении о порядке и способах информирования клиента о совершенных операциях с использованием электронного средства платежа (Приложение № 6).

7.3. Банк обязан предоставлять Клиенту необходимые рекомендации для работы с системой «iBank 2» путем размещения на информационных стендах в операционных залах и/или сайте Банка <http://www.bank-hlynov.ru/>.

7.4. Банк обязан передать Клиенту необходимые для работы программные модули системы «iBank 2» и средства подтверждения на возмездной основе до начала работы Клиента в системе «iBank 2». Факт передачи указанных средств фиксируется в актах передачи по форме Приложения № 9. [В случае обязательного использования USB-токенов].

7.5. Банк обязан предоставить Клиенту не менее одного аппаратного средства усиленной ЭП, необходимые рекомендации и системное программное обеспечение для использования устройства.

7.6. Банк обязан в случае получения от Клиента надлежащим образом заверенного уведомления о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента по форме Приложения № 8 заблокировать все ключи ЭП/средства подтверждения и прекратить обработку ЭД, подписанных/подтвержденных указанными средствами. Исполнение указанного уведомления производится Банком в срок, указанный Клиентом в уведомлении, но не ранее дня, следующего за днем получения уведомления. При наличии технической возможности, Банк может исполнить указанное уведомление в более короткий срок.

7.7. В случае получения от Клиента уведомления о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без

согласия Клиента, Банк обязан возместить Клиенту сумму операции, совершенной без согласия Клиента после получения указанного уведомления.

Возмещение Клиенту суммы операции производится на указанный Клиентом счет в срок не более 30 (тридцати) дней после проведения разбора конфликтной ситуации в соответствии с действующим на момент рассмотрения конфликтной ситуации Положением о процедуре разбора конфликтных ситуаций (Приложение № 4 к настоящему Договору) при условии подтверждения по результатам работы комиссии факта получения Банком соответствующего уведомления Клиента и совершения операции без согласия Клиента.

7.8. В случае неисполнения Банком обязанности по информированию Клиента о совершенной операции, Банк обязан возместить Клиенту сумму операции, о которой Клиент не был проинформирован, и которая была совершена без согласия Клиента.

Возмещение Клиенту суммы операции производится на указанный Клиентом счет в срок не более 30 (тридцати) дней после проведения разбора конфликтной ситуации в соответствии с действующим на момент рассмотрения конфликтной ситуации Положением о процедуре разбора конфликтных ситуаций (Приложение № 4 к настоящему Договору) при условии подтверждения по результатам работы комиссии факта неисполнения Банком обязанности по информированию Клиента об оспариваемой операции.

7.9. Банк обязан фиксировать полученные от Клиента уведомления о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента и подтверждать получение указанного уведомления, полученного на бумажном носителе, путем проставления на Клиентском экземпляре отметки о приеме уведомления.

7.10. Банк обязан хранить направленные клиенту и полученные от клиента уведомления о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента не менее трех лет.

7.11. Банк обязан рассматривать заявления/уведомления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом системы «iBank 2», а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений/уведомлений, в том числе в письменной форме по требованию Клиента, в срок, установленный настоящим Договором, но не более 30 (тридцати) дней со дня получения таких заявлений/уведомлений.

## **8. Совместные обязательства и ответственность Сторон**

8.1. Ответственность за достоверность информации и подлинность ЭП в ЭД несет Сторона, отправившая ЭД.

8.2. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами ключа ЭП Клиента, за исключением случаев, предусмотренных пунктами 7.7. и 7.8.

8.3. При расторжении настоящего Договора Стороны несут ответственность по всем ЭД, сформированным в системе «iBank 2», в соответствии с настоящим Договором и действующим законодательством РФ.

8.4. В случае возникновения конфликтных ситуаций между Клиентом и Банком при использовании системы «iBank 2», Стороны обязуются участвовать в рассмотрении споров в соответствии с действующим Положением о процедуре разбора конфликтных ситуаций (Приложение № 4 к настоящему Договору), выполнять требования, указанные в данном Положении и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. Действия Сторон согласно данному Положению являются обязательной составляющей процедуры досудебного урегулирования споров.

8.5. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием ЭСП, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу заинтересованной Стороны.

8.6. В случае недостижения Сторонами согласия, споры решаются в судебном порядке в соответствии с действующим законодательством РФ.

8.7. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств по настоящему Договору в случае возникновения обстоятельств непреодолимой силы. Обстоятельства непреодолимой силы понимаются в соответствии с п. 3 ст. 401 ГК РФ. Сторона, ссылающаяся на обстоятельства непреодолимой силы, обязана незамедлительно, но не позднее 48 (Сорока восьми) часов, информировать в письменной форме другую Сторону о наступлении и прекращении подобных обстоятельств и об их влиянии на возможность исполнить обязательство. Отсутствие уведомления возлагает на нарушившую Сторону обязанность возместить другой Стороне ущерб, который в случае своевременного уведомления мог быть предотвращен.

8.8. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате нарушения или ненадлежащего исполнения Клиентом требований по защите от Вредоносного кода рабочего места системы «iBank 2» (далее – Рабочее место).

## **9. Процедуры приема к исполнению, отзыва, возврата (аннулирования) распоряжений и порядок их выполнения**

9.1. Банк осуществляет прием ЭД, передаваемых по системе «iBank 2», круглосуточно. При невозможности передачи ЭД в Банк с использованием системы «iBank 2» Клиент может подать документы в Банк на бумажном носителе.

9.2. ЭД считается полученным Банком после присвоения ему в системе «iBank 2» статуса «Доставлен».

9.3. ЭД, поступивший в Банк, принимается к исполнению не позднее следующего рабочего дня за днем поступления.

9.4. При получении от Клиента ЭД, содержащего распоряжение, Банк производит следующие процедуры:

9.4.1. В автоматизированном режиме производится проверка подлинности ЭП сотрудника(-ов) Клиента в ЭД. При необходимости подтверждения ЭД одноразовым паролем, Банк в автоматизированном режиме проверяет правильность одноразового пароля.

При положительном результате проверок распоряжение считается произведенным уполномоченным лицом (лицами). Целостность распоряжения считается подтвержденной.

9.4.2. В автоматизированном режиме производится структурный контроль распоряжения и проверка правильности заполнения реквизитов распоряжения в соответствии с действующим законодательством и нормативными актами Банка России.

9.4.3. В автоматизированном режиме производится проверка достаточности денежных средств на расчётном счёте Клиента.

9.5. В случае положительного результата проведения проверок, указанных в п. 9.4., распоряжение принимается Банком к исполнению.

9.6. Распоряжение не принимается Банком к исполнению в случае отбраковки такого ЭД по критериям, указанным в п. 9.4. ЭД при этом аннулируется Банком.

9.7. Стороны признают надлежащим способ уведомления Клиента об аннулировании Банком распоряжений и иных ЭД путем присвоения статуса «Отвергнут», присвоенного ЭД в системе «iBank 2». В электронной форме документа Клиенту доступна информация, позволяющая идентифицировать аннулируемое распоряжение, дату его аннулирования и причину.

9.8. ЭД считается принятым Банком к исполнению после присвоения ему в системе «iBank 2» статуса «На обработке» («На исполнении»).

9.9. ЭД считается исполненным Банком после присвоения ему в системе «iBank 2» статуса «Исполнен».

9.10. Стороны признают надлежащим способ уведомления Клиента о получении и/или исполнении Банком распоряжений и иных ЭД путем присвоения соответствующего статуса

ЭД в системе «iBank 2». В электронной форме документа Клиенту доступна информация, содержащая реквизиты Банка, идентификатор системы «iBank 2», вид операции, дату операции, сумму операции, идентификатор операции с использованием системы «iBank 2», а также электронные отметки Банка об исполнении ЭД.

9.11. Характеристики переводов денежных средств: безотзывность, безусловность и окончательность трактуются в соответствии с действующим законодательством. Данные характеристики переводов денежных средств, осуществляемых Банком на основании распоряжений Клиентов, имеют следующие особенности:

9.11.1. Безотзывность перевода денежных средств наступает с момента списания денежных средств со счета плательщика.

9.11.2. Безусловность перевода денежных средств означает отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени.

Безусловность перевода денежных средств наступает:

при расчетах платежными требованиями - в случае предоставления Клиентом акцепта/заранее данного акцепта;

при расчетах инкассовыми поручениями - в случае наличия в договоре между Клиентом и Банком условия о списании денежных средств со счета Клиента и представлении Клиентом в Банк сведений о получателе средств, имеющем право предъявлять инкассовые поручения к счету Клиента.

9.11.3. Окончательность перевода денежных средств наступает:

при переводе денежных средств на счет получателя, открытый в Банке - в момент зачисления денежных средств на счет получателя средств;

при переводе на счета, открытые в иных банках - в момент зачисления денежных средств на счет банка получателя денежных средств.

9.12. Клиент вправе совершить отзыв распоряжения о переводе денежных средств до наступления момента безотзывности перевода, предоставив в Банк электронное заявление об отзыве распоряжения по форме, предусмотренной настройками системы «iBank 2», с возможностью указания причины отзыва документа. Заявление об отзыве служит основанием для отзыва Банком распоряжения.

9.13. Способом уведомления Клиента об отзыве распоряжения Стороны признают присвоенный ЭД в системе «iBank 2» статус «Отвергнут». В электронной форме документа Клиенту доступна информация, позволяющая идентифицировать аннулируемое распоряжение, дату его аннулирования и причину.

## **10. Порядок предоставления документов и информации, связанных с использованием ЭСП**

10.1. Клиент имеет право запрашивать у Банка документы, связанные с использованием электронного средства платежа:

10.1.1 копию договора об использовании электронного средства платежа;

10.1.2. копию руководства пользователя по использованию электронного средства платежа;

10.1.3. копию лицензии ФСБ РФ Банка на осуществление деятельности, связанной с использованием шифровальных (криптографических) средств;

10.1.4. копию акта разрешительной комиссии по участию в процедуре разбора конфликтной ситуации (если ранее между Клиентом и Банком проводилась процедура разбора конфликтной ситуации);

10.1.5. копию экспертного заключения о подлинности электронной подписи (если ранее в рамках разбора конфликтной ситуации проводилась экспертиза подлинности электронной подписи).

10.2. При необходимости Клиент направляет в Банк заявление в письменном виде в свободной форме с требованием о предоставлении одного или нескольких вышеуказанных документов.

10.3. Банк в течение 5 (Пяти) рабочих дней направляет Клиенту запрашиваемые им документы по адресу указанному в заявлении.

## **11. Стоимость услуг и порядок оплаты**

11.1. Стоимость использования Клиентом ЭСП рассчитывается согласно тарифам Банка, размещенным на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или сайте Банка <http://www.bank-hlynov.ru/>).

11.2. Оплата услуг по настоящему Договору производится путём списания денежных средств с расчетного счёта в российских рублях Клиента в безакцептном порядке.

11.3. В случае неоплаты Клиентом в срок стоимости услуг по настоящему Договору Банк вправе заблокировать использование ЭСП Клиентом без предварительного уведомления.

11.4. В случае блокирования Банком использования ЭСП Клиентом по основаниям, предусмотренным пунктом 11.3 настоящего Договора, повторное предоставление Клиенту возможности использования ЭСП производится после оплаты Клиентом задолженности по предоставленным услугам.

## **12. Срок действия Договора**

12.1. Настоящий Договор вступает в силу с момента подачи в Банк заявления о присоединении Клиента к настоящему Договору, составленного на бумажном носителе, и принятия заявления Банком.

12.2. Настоящий Договор считается заключенным на срок в 1 (Один) год и пролонгируется на каждый такой же срок, если ни одна из Сторон не изъявила желания расторгнуть настоящий Договор в порядке, установленном п. 13.1. Количество пролонгаций не ограничено.

### **13. Порядок изменения, расторжения Договора**

13.1. Каждая из Сторон вправе расторгнуть Договор в одностороннем порядке. Договор считается расторгнутым не ранее, чем через 30 (Тридцать) календарных дней после письменного уведомления об этом противоположной Стороны, в том числе направленным по системе «iBank 2». В случае расторжения Договора по инициативе Клиента, последний уведомляет Банк по форме Приложения № 10.

13.2. Внесение изменений и/или дополнений в настоящий Договор, в том числе утверждение Банком новой редакции настоящего Договора, производится Банком в одностороннем порядке.

13.3. Банк уведомляет Клиента об изменениях и/или дополнениях, вносимых в настоящий Договор, в том числе об утверждении Банком новой редакции настоящего Договора, за 5 (Пять) рабочих дней до даты введения изменений путем размещения их на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или сайте Банка <http://www.bank-hlynov.ru/>).

13.4. Банк уведомляет Клиента об изменениях тарифов Банка за 10 (Десять) рабочих дней до даты введения в действие новых Тарифов, путем размещения их на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или сайте Банка <http://www.bank-hlynov.ru/>).

13.5. В случае несогласия Клиента с изменениями и/или дополнениями, внесенными Банком в настоящий Договор, Клиент имеет право расторгнуть настоящий Договор в порядке, предусмотренном пунктом 13.1. настоящего Договора.

13.6. Договор считается расторгнутым автоматически в случае прекращения Договора банковского счета, заключенного между Клиентом и Банком, без письменного уведомления Банком Клиента или без письменного заявления Клиента.

### **14. Дополнительные условия.**

14.1. Подключение Клиентом дополнительных сервисных ресурсов, предоставляемых в рамках настоящего договора, производится на основании его заявления, по форме СОГЛАСНО Приложению №14».



**Приложение № 1**

К Договору об использовании электронного средства платежа

**УСЛОВИЯ (ПРАВИЛА)  
использования электронного средства платежа Система «iBank 2»**

В настоящих условиях (правилах) понятия Рабочее место и Вредоносный код используются в соответствии с Договором об использовании электронного средства платежа.

Во исполнение п. 3 статьи 9 Федерального закона «О национальной платежной системе» Банк настоящим информирует Клиента о следующем:

1. Использование клиентской части электронного средства платежа Система «iBank 2» (далее – Система) допускается из любых мест и любыми возможными способами с учетом указанных ниже ограничений.

2. Использование Системы не рекомендуется в следующих случаях (включая, но не ограничиваясь):

2.1. Клиентом не выполнены требования по защите от Вредоносного кода;

2.2. на Рабочем месте Клиента не установлены полученные из доверенных источников сертифицированные ФСБ средства криптографической защиты информации (СКЗИ);

2.3. Клиент не обеспечил надежное хранение и защиту от компрометации средств, используемых для дистанционного распоряжения счетом клиента (Средства подтверждения). К указанным средствам относятся:

- USB-токен или смарткарта «iBank 2 Key», содержащие ключ ЭП;
- файловое хранилище ключей ЭП;
- зарегистрированный в Системе мобильный телефон.

2.4. Клиент не ознакомился с правилами работы с Системой и правилами работы с СКЗИ;

2.5. Клиент не обеспечил периодическую (но не реже 1 раза в год) смену паролей для доступа к своему рабочему месту или к ключу ЭП;

2.6. Клиентом был обнаружен отказ специализированного ПО, используемого для защиты информации, или отказ клиентской части Системы;

2.7. Клиентом не обеспечен запрет использования на рабочем месте средств удаленного управления (R-Admin, TeamViewer и аналоги), администрирования и модификации ОС и её настроек (службы терминалов, удаленных рабочих столов и аналоги);

2.8. У клиента не настроен канал оповещения о совершенных операциях.

3. Клиент уведомлен, что при использовании Системы он несет повышенные риски, связанные с несанкционированным списанием средств клиента неуполномоченными лицами, в том числе и с использованием Вредоносного кода. Начиная работать с Системой, клиент подтверждает, что он полностью принимает на себя указанные риски.

4. Клиент несет полную ответственность за действия, совершенные третьими лицами, в случае передачи клиентом Средств подтверждения указанным лицам и/или в случае создания клиентом условий для несанкционированного использования третьими лицами Средств подтверждения. Клиент также несет полную ответственность за ущерб, причиненный Банку, указанными действиями или бездействием.

5. Клиент согласен с использованием логов (журналов) Системы и журналов модуля Системы по детектированию вредоносного программного обеспечения в качестве доказательства при разбирательстве по факту нарушений настоящих условий (правил) и требований по защите от Вредоносного кода.

**Приложение № 2**

К Договору об использовании электронного средства платежа

**ЗАЯВЛЕНИЕ**  
**о присоединении к договору об использовании электронного средства**  
**платежа**

Г. \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

Наименование Клиента:	
ИНН/КИО:	
ОГРН:	
Адрес места нахождения:	
Контактная информация:	
Контакты для информирования о совершенных операциях:	моб. тел.:

1. Клиент в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_, заявляет о присоединении к действующей в АО КБ «Хлынов» редакции Договора об использовании электронного средства платежа (ЭСП) и подтверждает, что все положения (условия) действующей в АО КБ «Хлынов» редакции Договора об использовании ЭСП (далее – Договор) ему известны и разъяснены в полном объеме.

2. Клиент подтверждает, что до заключения Договора проинформирован Банком об условиях использования ЭСП (Приложение № 1 к Договору) и иных условиях Договора, размещенных на общедоступных ресурсах Банка: информационных стендах в операционных залах и/или сайте Банка <http://www.bank-hlynov.ru/>. В частности Клиент проинформирован об ограничениях способов и мест использования, мерах безопасного использования ЭСП, случаях повышенного риска использования ЭСП, способах и сроках уведомления о совершении каждой операции с использованием ЭСП.

3. Клиент просит начать предоставление услуг в рамках Договора и подключить к системе «iBank 2» все счета, открытые в АО КБ «Хлынов» после предоставления Клиентом в Банк Сертификата ключа ЭП.

Приложения к данному Заявлению:

- а) Сертификат(ы) ключа ЭП
- б) Заявление «О регистрации средства подтверждения», либо заявление «Об отказе от использования дополнительного подтверждения электронных платежных документов в Системе «iBank2»:

**Отметка Клиента**

\_\_\_\_\_ (должность руководителя)

\_\_\_\_\_ (подпись)

\_\_\_\_\_ (Ф.И.О.)

М.П.

**Отметка Банка:**

Настоящее Заявление о присоединении к Договору об использовании ЭСП принято Банком.

« \_\_\_\_ » \_\_\_\_\_ 201\_\_ года

\_\_\_\_\_ (должность)

\_\_\_\_\_ (подпись)

\_\_\_\_\_ (Ф.И.О.)

М.П.

**Приложение № 3**

К Договору об использовании электронного средства платежа

**ЗАЯВЛЕНИЕ****о регистрации средства подтверждения**

г. \_\_\_\_\_ «\_\_\_» \_\_\_\_\_ 201\_\_ г.

Наименование Клиента:	
ИНН/КИО:	

Клиент просит Банк с «\_\_\_» \_\_\_\_\_ 201\_\_ г. зарегистрировать в системе «iBank 2» следующие номера мобильных телефонов в качестве средства получения одноразовых паролей:

## 1. Владелец ключа

ЭП Должность \_\_\_\_\_

Номера мобильных телефонов:

+7																			
+7																			
+7																			

## 2. Владелец ключа ЭП

Должность \_\_\_\_\_

Номера мобильных телефонов:

+7																			
+7																			
+7																			

## 3. Владелец ключа ЭП

Должность \_\_\_\_\_

Номера мобильных телефонов:

+7																			
+7																			
+7																			

Настоящим клиент \_\_\_\_\_ подтверждает принадлежность ему указанного(-ых) номера(-ов) мобильного(-ых) телефона(-ов) и дает согласие на получение в любое время суток одноразовых паролей на мобильный(-е) телефон(-ы) с вышеуказанным номером(-ами) одновременно.

Данное заявление носит отменяющий характер по отношению к любому ранее оформленному заявлению о регистрации Средств подтверждения.

**Требования к заполнению:** Заявление должно быть заполнено клиентом одним почерком и одной ручкой без исправлений, неиспользуемые поля должны быть заполнены прочерками.

Срок исполнения данного заявления – 3 рабочих дня при наличии ранее зарегистрированного ключа ЭП, а в случае его отсутствия – 3 рабочих дня с момента предоставления клиентом распечаток сертификата ключа ЭП.

\_\_\_\_\_ (должность руководителя)

\_\_\_\_\_ (подпись) М.П.

\_\_\_\_\_ (Ф.И.О.)

**Отметка Банка:**

Заявление исполнено " \_\_\_\_\_ " \_\_\_\_\_ 201\_\_ г.

\_\_\_\_\_ (должность)

\_\_\_\_\_ (подпись) М.П.

\_\_\_\_\_ (Ф.И.О.)

Номер заявки в IntraService – [ \_\_\_\_\_ ] (для внутреннего учета)

Управление корпоративного бизнеса

## Приложение № 4

К Договору об использовании электронного средства платежа

### ПОЛОЖЕНИЕ

#### о процедуре разбора конфликтной ситуации в рамках использования электронного средства платежа Система «iBank 2»

Настоящее положение о процедуре разбора конфликтной ситуации в рамках использования электронного средства платежа Система «iBank 2» (далее — Положение) в соответствии с Гражданским кодексом Российской Федерации, Федеральным Законом «О национальной платежной системе» и Федеральным Законом «Об электронной подписи», является порядком досудебного урегулирования споров между Банком и Клиентом возникающих из договора об использовании электронного средства платежа.

#### 1. Термины, применяемые в Положении

1.1. В рамках настоящего Положения используются понятия Электронное средство платежа (далее – ЭСП), Перевод денежных средств в соответствии с Федеральным Законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе».

1.2. В рамках настоящего Положения используются понятия Электронная подпись (далее – ЭП), Ключ электронной подписи (далее – Ключ ЭП), Ключ проверки электронной подписи (далее – Ключ проверки ЭП), Электронный документ (далее – ЭД) в соответствии с Федеральным Законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1.3. В рамках настоящего Положения используются понятия Сертификат ключа проверки электронной подписи (далее – Сертификат), Система «iBank 2», Пара ключей электронной подписи (далее – Пара ключей ЭП) в соответствии с Договором об использовании электронного средства платежа.

1.4. Термины, применяемые в рамках настоящего Положения, используются в следующих значениях:

- Конфликтная ситуация – спор между Клиентом и Банком по причине перевода денежных средств, в рамках которого Клиентом оспаривается подлинность электронной подписи в электронном документе и (или) факт уведомления о переводе денежных средств, возникшие в результате воздействия Вредоносного кода или по иным причинам.
- Разрешительная комиссия – орган, формируемый в соответствии с настоящим Положением с целью разбора Конфликтной ситуации по существу и документального оформления результатов работы.

#### 2. Состав Разрешительной комиссии

2.1. В обязательном порядке в состав Комиссии включаются представители Клиента и представители Банка.

2.2. По требованию Клиента и (или) Банка к работе Разрешительной комиссии может быть привлечен эксперт.

2.3. Эксперт может участвовать в работе Разрешительной комиссии непосредственно (лично). При этом эксперт включается в состав Разрешительной комиссии.

2.4. При невозможности непосредственного (личного) участия эксперта в работе Разрешительной комиссии, эксперт на основании полученных от Банка материалов проводит экспертизу подлинности ЭП или анализ архивов на предмет подтверждения факта уведомления Клиента. При этом эксперт не включается в состав Разрешительной комиссии.

2.5. Требования к эксперту определены в Разделе 8 настоящего Положения.

2.6. В качестве эксперта к работе Разрешительной комиссии может быть привлечен представитель разработчика Системы «iBank 2».

### 3. Порядок формирования Разрешительной комиссии

3.1. При возникновении Конфликтной ситуации, Клиент направляет в Банк заявление в письменном виде в свободной форме, которое должно содержать:

- дата и номер заявления;
- дата и номер заявления о присоединении к договору об использовании ЭСП;
- реквизиты Клиента (ИНН, адрес места нахождения, номер банковского счета);
- суть претензии с подробным изложением обстоятельств, на которых основана претензия, и сведений о подтверждающих ее доказательствах;
- обоснованный расчет заявленных в претензии требований;
- нормы законодательных и иных нормативных правовых актов, на которых основывается претензия;
- перечень прилагаемых к заявлению документов, составляющих доказательную базу (при наличии);
- список лиц, выступающих от лица Клиента в качестве членов Разрешительной комиссии.
- требование о привлечении к работе Разрешительной комиссии эксперта (при необходимости).

3.2. В случае привлечения по требованию Клиента к работе Разрешительной комиссии эксперта, Банк не позднее 2 (Двух) рабочих дней высылает в экспертную организацию запрос, содержащий:

- требования к экспертной организации;
- требования к эксперту;
- вопросы, поставленные перед экспертом;
- требуемый срок проведения экспертизы.

3.2.1. Экспертная организация в срок не позднее 2 (Двух) рабочих дней дает ответ Банку. В случае получения в указанный срок ответа от экспертной организации о соответствии предъявленным требованиям и возможности проведения экспертизы в указанный срок, Банк привлекает к работе Разрешительной комиссии указанного эксперта.

3.2.2. В случае неполучения от экспертной организации положительного ответа в указанный срок, Банк привлекает к работе Разрешительной комиссии представителя разработчика Системы «iBank 2».

3.3. Банк в течение 5 (Пяти) рабочих дней с момента получения заявления Клиента:

- определяет дату, время и место работы Разрешительной комиссии;
- формирует состав Разрешительной комиссии с учетом требований Клиента;
- информирует Клиента о назначенной дате, времени, месте работы Разрешительной комиссии и о ее составе.

3.4. Заседание Разрешительной комиссии должно быть организовано Банком не позднее 10 (Десяти) рабочих дней с момента получения заявления Клиента. В случае привлечения к работе Разрешительной комиссии эксперта, срок организации заседания Разрешительной комиссии продлевается на срок, необходимый эксперту для проведения экспертизы подлинности ЭП или

анализа архивов на предмет подтверждения факта уведомления Клиента.

3.5. В случае если Клиент не направит своих представителей для участия в работе Разрешительной комиссии, разбор Конфликтной ситуации осуществляется без представителей Клиента.

#### **4. Разбор Конфликтной ситуации, в рамках которой оспаривается подлинность электронной подписи**

4.1. При возможности доступа в ходе работы Разрешительной комиссии к базе данных системы «iBank 2», описанные ниже действия осуществляются с использованием штатного программного обеспечения Системы «iBank 2» АРМ «Операционист» и/или АРМ «Администратор».

4.2. При невозможности доступа в ходе работы Разрешительной комиссии к базе данных системы «iBank 2», описанные ниже действия осуществляются с использованием материалов, предварительно полученных (распечатанных, выгруженных) Банком из базы данных системы «iBank 2».

##### **Этап 1:**

4.3. Банк предъявляет на обозрение Разрешительной комиссии выписку по счету Клиента.

4.4. Клиент с помощью выписки по счету определяет оспариваемый перевод денежных средств.

4.5. Банк предъявляет ЭД, на основании которого совершен оспариваемый перевод денежных средств.

4.6. Разрешительная комиссия делает запись о факте предъявления/не предъявления Банком ЭД, при этом:

- В случае если Банк предъявляет ЭД, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 2 настоящего Раздела.
- В случае если Банк не предъявляет ЭД, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

##### **Этап 2:**

4.7. Разрешительная комиссия определяет Ключ ЭП, посредством которого был подписан ЭД.

4.8. Банк предъявляет на обозрение Разрешительной комиссии Сертификат, соответствующий вышеуказанному Ключу ЭП Клиента.

4.9. Разрешительная комиссия делает запись о факте предъявления/не предъявления Банком Сертификата, при этом:

- В случае если Банк предъявляет Сертификат, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 3 настоящего Раздела.
- В случае если Банк не предъявляет Сертификат Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

##### **Этап 3:**

4.10. Разрешительная комиссия просматривает ключ проверки ЭП, использующийся при проверке ЭП в ЭД, на основании которого совершен оспариваемый перевод денежных средств.

4.11. Разрешительная комиссия производит сверку шестнадцатеричного представления Ключа проверки ЭП, содержащегося в Сертификате, с шестнадцатеричным представлением Ключа проверки ЭП, используемого при проверке ЭП.

4.12. Разрешительная комиссия делает запись о факте наличия/отсутствия расхождения между шестнадцатеричным представлением Ключа проверки ЭП в Сертификате, и шестнадцатеричным представлением Ключа проверки ЭП, используемого при проверке ЭП, при этом:

- В случае если между шестнадцатеричными представлениями Ключей проверки ЭП расхождение не обнаружится, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 4 настоящего Раздела.
- В случае если обнаружится расхождение между шестнадцатеричными представлениями Ключей проверки ЭП, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

**Этап 4:**

4.13. Клиент предъявляет на обозрение Разрешительной комиссии уведомление о прекращении действия средства подтверждения и (или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента (при наличии).

4.14. Разрешительная комиссия определяет действительность Сертификата на момент получения Банком перевода денежных средств:

- Сертификат сверяется с оспариваемым переводом денежных средств. Предметом сверки выступают даты начала и окончания действия Сертификата и дата получения Банком от Клиента распоряжения на осуществление перевода денежных средств. При необходимости может учитываться и время указанных событий.
- Уведомление о прекращении действия средства подтверждения и (или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента (при наличии) сверяется с оспариваемым переводом денежных средств. Предметом сверки выступают дата отметки о принятии (об исполнении) Банком указанного уведомления и дата получения Банком от Клиента распоряжения на осуществление перевода денежных средств. При необходимости может учитываться и время указанных событий, а также время, необходимое Банку на исполнение указанного уведомления.

4.15. Разрешительной комиссией делается запись о действительности/недействительности Сертификата на момент получения Банком от Клиента распоряжения на перевод денежных средств, при этом:

- В случае действительности Сертификата на момент получения Банком от Клиента распоряжения на осуществление перевода денежных средств, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 5 настоящего Раздела.
- В случае недействительности Сертификата на момент получения Банком от Клиента распоряжения на осуществление перевода денежных средств, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

**Этап 5:**

4.16. Разрешительная комиссия проводит проверку подлинности ЭП в ЭД.

4.17. Разрешительной комиссией может использоваться специализированная утилита от разработчика Системы «iBank 2» для автономной проверки подлинности ЭП.

4.18. Разрешительной комиссией делается запись о подлинности/нарушении подлинности ЭП в ЭД, при этом Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

### **5. Разбор Конфликтной ситуации, в рамках которой оспаривается факт уведомления о переводе денежных средств (о совершенной операции)**

#### **Этап 1:**

5.1. Банк предъявляет на обозрение Разрешительной комиссии выписку по счету Клиента.

5.2. Клиент с помощью выписки по счету определяет оспариваемый перевод денежных средств.

5.3. Банк предъявляет Разрешительной комиссии архивы уведомлений, переданных в период, включающий дату получения Банком от Клиента распоряжения на осуществление перевода денежных средств. Банком могут по его усмотрению и в зависимости от технической возможности использоваться архивы уведомлений, хранящиеся в базе данных и журналах Системы «iBank 2», и (или) архивы уведомлений, полученные от оператора связи, предоставляющего услугу по передаче уведомлений.

5.4. Банк определяет в архиве уведомление, соответствующее рассматриваемому переводу денежных средств.

5.5. Комиссия определяет реквизиты, по которым было направлено уведомление. При использовании для информирования Клиента изменения поля «Статус» и выписки в Системе по счету Клиента, данный пункт не рассматривается.

5.6. Банк предъявляет действовавший на момент осуществления перевода и заверенный Клиентом документ, в котором указаны реквизиты для информирования Клиента (информация для связи с Клиентом).

5.7. Клиент предъявляет действовавший на момент осуществления перевода документ с отметкой Банка, в котором указаны реквизиты для информирования Клиента (информация для связи с Клиентом) при наличии такого документа.

5.8. Разрешительная комиссия делает запись о факте соответствия/не соответствия реквизитов, по которым было отправлено уведомление, реквизитам, указанным Клиентом для осуществления информирования:

- В случае если реквизиты, по которым было совершено информирование Клиента, соответствуют реквизитам, указанным Клиентом для осуществления информирования, Конфликтная ситуация рассматривается далее по существу. Разрешительная комиссия переходит к Этапу 2 настоящего Раздела.
- В случае если реквизиты не соответствуют, Конфликтная ситуация далее по существу не рассматривается. Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

#### **Этап 2:**

5.9. Комиссия определяет срок отправки уведомления. При рассмотрении архивов, хранящихся в базе данных системы «iBank 2», может использоваться АРМ «Операционист».

5.10. В случае использования для информирования Клиента изменения поля «Статус», по истории документа определяется момент присвоения ЭД статуса «На обработке»/«На исполнении».

5.11. В случае использования для информирования Клиента выписки в Системе по счету Клиента, по распечатанной проводке определяется момент подписи проводки (информации об операции), который соответствует моменту появления данной информации в выписке по



счету Клиента.

5.12. Разрешительная комиссия делает запись о соблюдении/не соблюдении срока отправки уведомления (информирования Клиента), при этом Разрешительная комиссия переходит к Разделу 6 настоящего Положения.

## **6. Подведение итогов разбора Конфликтной ситуации**

6.1. По результатам работы Разрешительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

6.2. Помимо изложения выводов и решения Разрешительной комиссии в акте должны содержаться:

- состав Разрешительной комиссии;
- дата и место составления акта;
- дата, время начала и окончания работы Разрешительной комиссии;
- фактические обстоятельства, послужившие основанием возникновения претензии;
- краткий перечень мероприятий, проведенных Разрешительной комиссией;
- реквизиты оспариваемого ЭД;
- вывод о подлинности/нарушении подлинности ЭП в оспариваемом ЭД и его обоснование  
– в случае оспаривания Клиентом подлинности ЭП;
- вывод об уведомлении/не уведомлении Клиента о совершенной операции - в случае оспаривания Клиентом факта уведомления о переводе денежных средств;
- указание на особое мнение члена Разрешительной комиссии (при наличии);
- собственноручные подписи членов Разрешительной комиссии.

6.3. В случае если проводилась экспертиза подлинности ЭП или анализ архивов на предмет подтверждения факта уведомления Клиента, к акту прилагается подготовленное экспертом заключение о подлинности ЭП или результат анализа архивов соответственно.

6.4. Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению Разрешительной комиссией, в двух экземплярах по экземпляру для Клиента и Банка и подписывается всеми членами Разрешительной комиссии. В случае включения в состав Разрешительной комиссии эксперта, акт составляется в трех экземплярах.

6.5. Решение Разрешительной комиссии по результатам разбора Конфликтной ситуации, в рамках которой оспаривается подлинность электронной подписи:

6.5.1. Разрешительная комиссия признает Банк исполнившим платеж без согласия Клиента, и Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

- Банк не предъявляет ЭД, подписанный Клиентом, на основании которого Банк совершил перевод денежных средств Клиента.
- Банк не предъявляет Сертификат, соответствующий Ключу ЭП Клиента, которым был подписан ЭД.
- В случае обнаружения расхождения между шестнадцатеричным представлением Ключа проверки ЭП в Сертификате, и шестнадцатеричным представлением Ключа проверки ЭП, использующегося при проверке ЭП.

- Сертификат был недействительным на момент получения Банком от Клиента распоряжения на осуществление перевода денежных средств.
- Хотя бы одна ЭП Клиента в ЭД оказалась не подлинной.

6.5.2. В иных случаях, за исключением определенных в пункте 6.5.1., Банк не несет ответственности перед Клиентом за совершение перевода денежных средств.

6.6. Решение Разрешительной комиссии по результатам разбора Конфликтной ситуации, в рамках которой оспаривается факт уведомления о переводе денежных средств (о совершенной операции):

6.6.1. Разрешительная комиссия признает Банк не исполнившим обязанность по информированию Клиента о совершенной операции, и Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

- Банк осуществил информирование Клиента о платеже (операции) по реквизитам, не соответствующим реквизитам, указанным Клиентом для осуществления информирования.
- Банк осуществил информирование Клиента о платеже (операции) в срок, превышающий срок, установленный в Договоре.

6.6.2. В иных случаях, за исключением определенных в пункте 6.6.1, Банк признается Разрешительной комиссией исполнившим обязанность по информированию Клиента не несет ответственности перед Клиентом за совершение перевода денежных средств.

6.7. Расходы по формированию и работе Разрешительной комиссии, исключая расходы Клиента, связанные с привлечением им в одностороннем порядке независимых экспертов, возлагаются на Банк. В случае признания Разрешительной комиссией требований Клиента необоснованными, Клиент обязан в течение 7 рабочих дней с даты составления Акта возместить Банку все указанные расходы. При нарушении Клиентом указанного выше условия, Банк имеет право взыскать указанные расходы путем безакцептного списания средств с любого счета Клиента, открытого в Банке.

## **7. Проверка подлинности электронной подписи экспертом**

7.1. По требованию Клиента и (или) Банка проведение проверки подлинности ЭП в ЭД может быть поручено экспертной организации.

7.2. При наличии требования о проверке подлинности ЭП в ЭД экспертной организацией Банк в течение (Пяти) рабочих дней с момента получения заявления Клиента или с момента принятия решения о проведении экспертизы по собственной инициативе, направляет эксперту следующие материалы:

- файлы, полученные в результате выгрузки спорного ЭД из базы данных системы «iBank 2»;
- заверенную копию Сертификата;
- в случае проведения экспертизы по инициативе Клиента - копию заявления Клиента, указанного в пункте 2.1 настоящего Положения.

7.3. По результатам экспертизы подлинности ЭП организация формирует заключение о подлинности ЭП в предоставленном ЭД и высылает его в адрес Банка.

7.4. Срок проведения экспертизы подлинности ЭП не должен превышать 10 (Десяти) рабочих дней с момента получения экспертной организацией всех необходимых материалов.

7.5. В случае принятия решения о проведении экспертизы подлинности ЭП в ЭД экспертом, срок организации заседания Разрешительной комиссии увеличивается на срок, необходимый эксперту для проведения экспертизы подлинности ЭП.

## **8. Требования к эксперту, экспертной организации и экспертному заключению**

### **8.1. Экспертная организация должна:**

- использовать на законных основаниях для проверки сертифицированные ФСБ РФ ЭП шифровальные (криптографические) средства, реализующие криптографические процедуры проверки ЭП и криптографическую процедуру вычисления хеш-функции по действующим ГОСТам Российской Федерации;
- использовать на законных основаниях для проверки ЭП программное обеспечение, разработанное организацией имеющей лицензию ФСБ РФ на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем, если для проверки ЭП используется Программное обеспечение разработанное сторонней организацией, и (или) иметь лицензию ФСБ России на разработку защищенных с использованием шифровальных (криптографических) средств информационных систем, если для проверки ЭП используется программное обеспечение собственной разработки.

### **8.2. Эксперт должен:**

- иметь высшее профессиональное образование в области информационной безопасности или пройти переподготовку по одной из специальностей этого направления в объеме не менее 500 часов;
- иметь стаж работы в области информационной безопасности не менее 5 (Пяти) лет.

### **8.3. Заключение о проверке подлинности должно:**

- быть оформленным в форме экспертного заключения;
- содержать сведения об Экспертной организации: фирменное наименование, место нахождения, ИНН, КПП, ОГРН;
- содержать контактные данные Экспертной организации: телефон, факс, e-mail;
- содержать дату оформления (составления);
- содержать время и дату проведения исследования, адрес места проведения исследования, основание проведения исследования;
- содержать перечень вопросов поставленных на разрешение эксперту;
- содержать перечень объектов исследования представленных эксперту;
- содержать методику исследования;
- содержать результаты исследования;
- содержать выводы эксперта;
- быть заверенным подписью эксперта, подписью единоличного исполнительного органа экспертной организации и печатью экспертной организации.

**Приложение № 5**

К Договору об использовании электронного средства платежа

**ПЕРЕЧЕНЬ**

**электронных документов передаваемых по Системе «iBank 2»**

	<b>Наименование Электронного документа</b>
1	Платежное поручение
2	Заявление на перевод иностранной валюты
3	Поручение на обязательную продажу
4	Поручение на продажу иностранной валюты
5	Поручение на покупку иностранной валюты
6	Поручение на списание валюты с транзитного счета
7	Поручение на конвертацию иностранной валюты
8	Справка о валютных операциях
9	Паспорт сделки по контракту
10	Паспорт сделки по кредитному договору
11	Письмо
12	Зарплатный реестр
13	Заявление на открытие карты
14	Заявление на присоединение к зарплатному проекту
15	Заявление на перевыпуск банковской карты
16	Изменение сведений о сотруднике
17	Заявление на открепление от зарплатного проекта
18	Реестры совершенных платежей

## Приложение № 6

К Договору об использовании электронного средства платежа

### ПОЛОЖЕНИЕ

#### о порядке и способах информирования клиента о совершенных операциях с использованием электронного средства платежа

##### 1. Способы информирования Клиента

В целях исполнения требований Федерального закона от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» Банк осуществляет информирование Клиента о совершенных операциях посредством направления уведомлений одним из способов:

1.1. Путем отправки SMS-сообщения на указанный Клиентом номер (номера) мобильного телефона, зарегистрированного в РФ.

Обязанность банка по информированию Клиента считается исполненной Банком при направлении SMS-сообщения о совершенной операции на номер мобильного телефона, указанный Клиентом. Уведомление считается полученным Клиентом с момента отправки Банком SMS-сообщения.

1.2. Путем отправки письма-уведомления Клиенту в систему «iBank 2».

Обязанность Банка по информированию Клиента считается исполненной Банком при направлении сообщения Клиенту в систему «iBank 2» о совершении операции. Уведомление считается полученным Клиентом с момента отправки Банком сообщения в систему «iBank 2».

1.3. Путем изменения статуса соответствующего электронного документа в системе «iBank 2». Присвоение электронному документу в системе «iBank 2» статуса «Доставлен» подтверждает получение Банком распоряжения Клиента. Присвоение электронному документу в системе «iBank 2» статуса «На обработке»/«На исполнении» подтверждает прием Банком распоряжения Клиента к исполнению. Присвоение электронному документу статуса «Исполнено» подтверждает исполнение Банком распоряжения Клиента. Присвоение электронному документу статуса «Отвергнут» подтверждает аннулирование Банком распоряжения Клиента.

Обязанность Банка по информированию Клиента считается исполненной Банком при изменении статуса электронного документа в системе «iBank 2». Уведомление считается полученным Клиентом с момента изменения статуса электронного документа в системе «iBank 2».

1.4. Банк обязан проинформировать Клиента о совершенных операциях с использованием ЭСП не позднее дня, следующего за днем исполнения соответствующей операции.

1.5. Способы информирования, указанные в п.1.3. применяются Банком для информирования Клиента о:

- получении Банком распоряжения на осуществление перевода денежных средств [при информировании Клиента о получении ЭД статуса «Доставлен»];
- принятии Банком распоряжения на осуществление перевода денежных средств к исполнению [при информировании Клиента о получении ЭД статуса «На обработке»/«На исполнении»];
- исполнении Банком распоряжения на осуществление перевода денежных средств [при информировании Клиента о получении ЭД статуса «Исполнен»];
- аннулировании Банком распоряжения на осуществление перевода денежных средств [при информировании Клиента о получении ЭД статуса «Отвергнут»].

1.6. Способ информирования, указанный в п. 1.1, 1.2. применяется Банком для

информирования Клиента о:

- принятии Банком распоряжения на осуществление перевода денежных средств к исполнению [при использовании предварительной выписки];
- исполнении Банком распоряжения на осуществление перевода денежных средств.

1.7. Получение уведомления считается подтвержденным Клиентом в случае отсутствия сообщений от Клиента о неполучении уведомления в срок не позднее двух часов после совершения операции.

## **2. Порядок информирования Клиента**

2.1. При информировании Клиента путем отправки SMS-сообщений и/или сообщений в системе «iBank 2», Стороны руководствуются приведенными ниже положениями.

2.2. Уведомление в виде сообщения в системе «iBank 2» может включать:

- 1) наименование Банка;
- 2) идентификатор электронного средства платежа;
- 3) вид операции;
- 4) дата операции;
- 5) сумма операции;
- 6) валюта операции;
- 7) дополнительная информация о контрагенте;
- 8) идентификатор устройства при его применении для осуществления операции с использованием электронного средства платежа;
- 9) иная информация.

2.3. Уведомление в виде SMS-сообщения может включать:

- 1) указание расчётного счёта клиента, замаскированного в формате "\*12345", где 12345 - последние пять цифр номера расчётного счёта клиента;
- 2) дату операций, в формате "ДД.ММ.ГГГГ";
- 3) количество расходных операций в Интернет-банке за указанную дату;
- 4) сумму расходных операций в Интернет-банке, в рублях за указанную дату.

## **3. Права и обязанности Сторон**

3.1. Клиент обязан предоставить Банку достоверную информацию для связи с Клиентом.

3.2. Клиент обязан предоставить в Банк письменное заявление в случае изменения номера мобильного телефона. Все риски, связанные с несвоевременным предоставлением информации об изменении номера мобильного телефона, несет Клиент. Обязанность Банка по информированию клиента считается исполненной надлежащим образом при направлении сообщений на ранее известный номер мобильного телефона, если на дату отправки таких сообщений Банк не получил заявление Клиента об изменении номера мобильного телефона.

3.3. Клиент обязан не реже одного раза в сутки проверять поступающие сообщения в систему «iBank 2» и/или на номер мобильного телефона SMS-сообщения о совершенной операции, проверять информацию о совершенной операции, размещаемую Банком в системе «iBank 2», получать выписки о совершенных операциях в подразделении Банка.

3.4. Клиент обязан самостоятельно обеспечить поддержку функции приема SMS-

сообщений на своем мобильном телефоне.

3.5. Клиент обязан самостоятельно и за свой счет поддерживать баланс средств на лицевом счете у оператора мобильной связи, необходимый для обеспечения непрерывности получения SMS-сообщений о совершенных операциях.

3.6. Клиент обязан самостоятельно обеспечить доступность получения SMS-сообщений у своего оператора мобильной связи при нахождении мобильного телефона в междугородном или международном роуминге.

3.7. Если для информирования Клиента об операции используется изменение поля «Статус». Клиент обязан просматривать список ЭД в системе «iBank 2» не реже, чем один раз в день.

3.8. Если для информирования Клиента об операции используется выписка по счету. Клиент обязан запрашивать в системе «iBank 2» выписки за предыдущий день по открытым в Банке счетам не реже, чем один раз в день.

3.9. Клиент вправе в любой момент изменить номер телефона, на который осуществляется уведомление в виде SMS-сообщения, предоставив Банку обновленную информацию для связи с Клиентом и направления ему уведомлений, установленным Банком способом.

3.10. Банк имеет право проводить работы по техническому обслуживанию программно-аппаратных средств, обеспечивающих отправку сообщений. На период проведения указанных мероприятий отправка сообщений Клиентом может быть временно приостановлено.

#### **4. Ответственность сторон**

4.1. В случае не предоставления Клиентом в Банк достоверной информации о номере мобильного телефона, Клиент признается не предоставившим надлежащим образом информацию для связи с Клиентом, и Банк вправе заблокировать доступ Клиента к системе «iBank 2» и/или расторгнуть договор с Клиентом.

4.2. В случае если Клиент предоставил неверные сведения о номере мобильного телефона для осуществления Банком информирования о совершенных операциях и/или номер мобильного телефона не используется (блокирован/отключен и др.), Банк не несет ответственности за неисполнение обязанности по направлению уведомления Клиенту.

4.3. Банк не несет ответственности в случае неполучения Клиентом SMS-сообщения о совершенной операции, не осуществления просмотра Клиентом в системе «iBank 2» списка ЭД и(или) выписок за текущий и предыдущий день по открытым в Банке счетам.

#### **5. Иные условия**

5.1. Клиент согласен на передачу информации, связанной с операциями по его счету, путем отправки SMS-сообщений и сообщения в систему «iBank 2». Клиент дает свое согласие на передачу информации о номере мобильного телефона третьим лицам в целях информирования о совершенных операциях.

**Приложение № 7**

К Договору об использовании электронного средства платежа

**ПОЛОЖЕНИЕ****о порядке действий сторон в случае компрометации средства подтверждения**

1. События, которые могут быть расценены как компрометация Средства подтверждения:

1.1. утрата/хищение Средства подтверждения ;

1.2. несанкционированное копирование ключа ЭП;

1.3 передача ключа ЭП по открытым каналам связи;

1.4. случаи, когда нельзя достоверно установить, что произошло со Средством подтверждения (в том числе случаи, когда Средство подтверждения вышло из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника);

1.5. любые другие признаки осуществления несанкционированных действий в системе «iBank 2».

2. Решение о компрометации Средства подтверждения может быть принято владельцем ключа ЭП или руководителем организации.

3. В случае компрометации Средства подтверждения Клиенту необходимо:

3.1. немедленно прекратить любые действия с рабочим местом Системы «iBank 2», обесточить его и отключить от информационных сетей или перевести в режим гибернации;

3.2. произвести фотосъемку Рабочего места, обеспечить его сохранность, поместив в место с ограниченным доступом и обеспечив при этом защиту от вскрытия. При необходимости ведения хозяйственной деятельности - задействовать другое Рабочее место;

3.3. обратиться в Банк с уведомлением о компрометации Средства подтверждения по форме Приложения № 8 не позднее дня, следующего за днем получения уведомления о совершенной операции, и просьбой заблокировать указанные Средства подтверждения и остановить обработку ЭД, подписанных/подтвержденных указанными Средства подтверждения;

3.4. обратиться в иные банки, которые предоставляют Клиенту услуги электронного банкинга, с просьбой о внеплановой замене ключей ЭП в их информационных системах;

3.5. предпринять меры для обеспечения сохранности и неизменности записей с внутренних и внешних камер систем видеонаблюдения, журналов систем контроля доступа, средств обеспечения и разграничения доступа в сеть Интернет за максимальный период времени;

3.6. провести сбор записей с межсетевых экранов и других средств защиты информации, коммуникационного оборудования и устройств, которые могут использоваться для удаленного управления Рабочим местом;

3.7. обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений Рабочего места или локальной вычислительной сети компании с сетью Интернет;

3.8. не предпринимать никаких действий для поиска и удаления компьютерных вирусов, восстановления работоспособности Рабочего места, не отправлять Рабочее место в сервисные службы для восстановления работоспособности;

3.9. зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к Рабочему месту, предпринимаемые действия с Рабочим местом, подготовить объяснения ответственных сотрудников в случае использования Рабочего



места в целях, отличных от осуществления операций в системе электронного банкинга, посещаемых сайтах, перебоях в работе или отказах Рабочего места, обращениях в службы сопровождения, в Банк, о сторонних лицах, побывавших в месте расположения Рабочего места и т.д.

3.10. все действия с Рабочим местом производить коллегиально, протоколировать и документировать, в том числе с использованием фотосъемки.

4. О компрометации ключа ЭП Клиент уведомляет Банк следующими способами:

4.1. по телефону +7(800) 250-2-777. Клиент уведомляет сотрудника Банка, при этом идентификация Клиента осуществляется по Блокировочному слову. Клиент заполняет Уведомление о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента по утвержденной форме (далее - Уведомление) и незамедлительно отправляет его в Банк. Банк не позднее 1 часа с момента обращения Клиента по телефону и подтверждения его полномочий останавливает обработку ЭД, подписанных указанными ключами ЭП, и блокирует указанные ключи ЭП на срок не более 4 часов. В случае неполучения Банком от Клиента в указанный срок оригинала Уведомления, Банк имеет право любым способом запросить у Клиента подтверждение факта обращения в Банк и/или продолжить обработку ЭД, подписанных указанными ключами ЭП, и/или разблокировать указанные Клиентом ключи ЭП.

4.2. Клиент передает оригинал Уведомления в отделение банка, в котором обслуживается. Банк не позднее дня, следующего за днем получения оригинала Уведомления, останавливает обработку ЭД, подписанных указанным в Уведомлении ключом ЭП, и блокирует указанные ключи ЭП. При наличии технической возможности, Банк может исполнить указанное уведомление в более короткий срок.

5. Электронные документы, находящиеся на момент получения/исполнения Уведомления в статусе «На обработке»/«На исполнении» отзыву не подлежат.

**Приложение № 8**

К Договору об использовании электронного средства платежа

**УВЕДОМЛЕНИЕ****о прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании ЭСП без согласия Клиента**

г. \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Наименование Клиента:	
ИНН/КИО:	

Настоящим уведомляю Банк о:

- прекращения действия средства подтверждения,  
 об утрате/компрометации средства подтверждения  
 использовании ЭСП без согласия Клиента.

Прошу с ЧЧ: ММ ХХ.ХХ.ХХХХ заблокировать указанные ниже средства подтверждения, использовавшиеся в рамках Договора об использовании ЭСП с ОАО КБ «Хлынов» согласно заявлению о присоединении № ХХХ от ХХ.ХХ.ХХХХ., и остановить обработку ЭД, подписанных/подтвержденных указанными средствами:

- USB-токен/смарт-карта «iBank 2 Key» № \_\_\_\_\_;  
 файловое хранилище ключа ЭП,

содержащий(-ее) следующие ключи ЭП:

Ф.И.О. владельца	Идентификатор ключа проверки ЭП

- мобильный телефон:

Ф.И.О. владельца	Номер телефона

\_\_\_\_\_ (\_\_\_\_\_) (должность руководителя) (подпись) (Ф.И.О.)

М.П.

**Отметка Банка:**

Уведомление принято к исполнению в Банке " \_\_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_ (\_\_\_\_\_) (должность) (подпись) (Ф.И.О.)

М.П.

**Приложение № 9**

К Договору об использовании электронного средства платежа

**АКТ № X****передачи программных средств, средств усиленной ЭП, средств подтверждения и сопроводительной документации**

г. \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Коммерческий банк "ХЛЫНОВ" (открытое акционерное общество), именуемое в дальнейшем «Банк» в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_, с одной стороны, и \_\_\_\_\_, именуемое в дальнейшем «Клиент», в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», принимая во внимание Договор об использовании ЭСП, составили настоящий Акт о нижеследующем:

Банком надлежащим образом переданы, а Клиентом получены следующие Средства подтверждения:

UBS-токен/смарт-карта «iBank 2 Key» № \_\_\_\_\_;

Банком надлежаще передан, а Клиентом получен носитель Рег. № XXXX со следующими программными средствами и документацией:

- дистрибутив программы для ЭВМ «РС-Банкинг»;
- программное средство усиленной ЭП СКЗИ «Крипто-КОМ 3.3» № 508А-001067/XXXX/XXX;
- программное средство усиленной ЭП ПБЗИ «Крипто-Си» № 628-001002/XXXX/XXX;
- драйвер для Аппаратного средства усиленной ЭП USB-токен/смарт-карта «iBank 2 Key»;
- документация к СКЗИ (ПБЗИ);
- документация по использованию Средств подтверждения.

В случае изменений версий драйвера для Аппаратного средства усиленной ЭП «iBank 2 Key» актуальные версии драйвера могут быть загружены с сайта разработчика <https://ibank2.ru>.

Настоящий Акт составлен в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

БАНК

КЛИЕНТ

\_\_\_\_\_  
(подпись) (Ф.И.О.)

\_\_\_\_\_  
(подпись) (Ф.И.О.)

М.П.

М.П.

**Приложение № 10**

К Договору об использовании электронного средства платежа

**УВЕДОМЛЕНИЕ  
о приостановлении/прекращении использования ЭСП**

Г. \_\_\_\_\_ «\_\_» \_\_\_\_\_ 20\_\_ г.

Наименование Клиента:	
ИНН/КИО:	

Уведомляет Банк о приостановлении/прекращении использования ЭСП использовавшихся в рамках договора об использовании ЭСП с ОАО КБ «Хлынов» согласно заявлению о присоединении № XXX от XX.XX.XXXX.

Прошу с 00:00 XX.XX.201X г. заблокировать все ключи ЭП и Средства подтверждения и прекратить обработку электронных документов, подписанных/подтвержденных указанными средствами.

\_\_\_\_\_  
(должность руководителя) (подпись) (Ф.И.О.)

М.П.

**Отметка Банка:**

Уведомление принято к исполнению в Банке "\_\_\_\_\_" \_\_\_\_\_ 201\_ г.

\_\_\_\_\_  
(должность) (подпись) (Ф.И.О.)

М.П.

**Приложение № 11**

К Договору об использовании электронного средства платежа

**ЗАЯВЛЕНИЕ  
на IP-фильтрацию при работе в Системе «iBank 2»**

г. \_\_\_\_\_

«\_\_» \_\_\_\_\_ 20\_\_ г.

Наименование Клиента:	
ИНН/КИО:	

Настоящим заявляю о доступе к системе «iBank 2», только со следующих (-их) IP-адреса (-ов):

№ п/п	IP-адрес*				Маска IP-адрес*
1					
2					
3					
4					
5					
6					
7					

\* Может быть указан либо IP-адрес (-а), либо маска IP-адреса (-ов), с которого (-ых) будет осуществляться соединение по Системе «iBank 2»

Прошу установить фильтр IP-адресов по следующим регионам:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_
4. \_\_\_\_\_

Настоящим отказываюсь от осуществления IP-фильтрации. Риски, связанные с таким отказом, мне разъяснены.

**Отметка Клиента:**

\_\_\_\_\_ (должность руководителя) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.

**Отметка Банка:**

Заявление принято к исполнению в Банке " \_\_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.

**Приложение № 12**

К Договору об использовании электронного средства платежа

**ЗАЯВЛЕНИЕ****на подключение услуги многофакторной аутентификации в Системе «iBank 2»**

Г. \_\_\_\_\_

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

«Клиент», в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_, принимая во внимание Договор об использовании ЭСП, составил настоящее заявление о нижеследующем:

Для повышения уровня безопасности Клиент выбирает следующие источники многофакторной аутентификации с использованием одноразовых паролей при входе в систему «iBank 2»:

тел. № +7 \_\_\_\_\_;

**Отметка Клиента:**

\_\_\_\_\_ (\_\_\_\_\_)  
 (должность руководителя) (подпись) (Ф.И.О.)

М.П.

**Отметка Банка:**

Заявление принято к исполнению в Банке " \_\_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_ (\_\_\_\_\_)  
 (должность) (подпись) (Ф.И.О.)

М.П.

**Приложение № 13**

К Договору об использовании электронного средства платежа

**ТРЕБОВАНИЯ****по защите от Вредоносного кода рабочего места Системы «iBank 2»**

К средствам защиты от Вредоносного кода относятся средства, используемые для:

- выявления и обезвреживания вредоносного кода (антивирусы);
- межсетевого экранирования Рабочего места или корпоративной сети;
- Web-фильтрации;
- обнаружения и предотвращения вторжений;
- контроля выполнения приложений.

Для обеспечения надлежащей защиты от вредоносного кода Клиент обязан:

1. обеспечить непрерывное использование средств защиты от Вредоносного кода;
2. обеспечить периодический контроль целостности системного, прикладного и специального программного обеспечения;
3. ежедневно осуществлять проверку Рабочего места на наличие Вредоносного кода;
4. обеспечить регулярное обновление средств защиты от Вредоносного кода, обновление прикладного программного обеспечения, установку пакетов обновления безопасности операционной системы;
5. использовать лицензионное программное обеспечение или программное обеспечение, полученное исключительно из доверенных источников;
6. использовать для работы в Системе учетную запись, не входящую в группу «Локальные администраторы» или аналогичную группу пользователей;
7. осуществлять вход в сеть Интернет с Рабочего места исключительно для подключения к сайту Банка;
8. ограничивать по времени доступ ответственных лиц к ключу электронной подписи (токену) и/или телефону, на который приходят SMS – подтверждения платежей;
9. контролировать суммы переводов через предоставляемую банком бесплатную услугу СМС-подтверждения, отвергать сверхлимитные платежи; контролировать реквизиты получателей.

## Приложение №14

к Договору об использовании электронного средства платежа

### ЗАЯВЛЕНИЕ для подключения модуля «iBank 2 для 1С:Бухгалтерии»

г. \_\_\_\_\_ « \_\_\_\_\_ » \_\_\_\_\_ 20  
\_\_\_\_\_ г.

Наименование Клиента:	
ИНН/К/ИО:	

Сведения о владельце ключа \_\_\_\_\_  
(фамилия, имя, отчество

полностью) Прошу предоставить доступ к модулю «iBank 2 для

1С:Бухгалтерии». **Отметка Клиента:**

\_\_\_\_\_  
(должность руководителя) \_\_\_\_\_ (подпись) (Ф.И.О.)

М.П.

**Отметка Банка:**

Заявление принято к исполнению в Банке " \_\_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_  
(должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.



**Приложение № 15**  
К Договору об использовании  
электронного средства платежа

**ЗАЯВЛЕНИЕ**  
на настройку ограничений при работе в системе «iBank 2»

г. \_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Наименование Клиента:	
ИНН:	

Настоящим заявлением прошу установить следующие ограничения на работу в системе «iBank2» по расчетному счету:

Р/с № 

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

- Время приема п/п к исполнению: с \_\_\_\_ : \_\_\_\_ до \_\_\_\_ : \_\_\_\_
- Максимальная сумма перевода: \_\_\_\_\_ руб.
- Установить перечень возможных получателей:

№ п/п	БИК	Счет

**Отметка Клиента:**

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.

**Отметка Банка:**

Заявление принято к исполнению в Банке " \_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.

Заявление исполнено Банком " \_\_\_\_ " \_\_\_\_\_ 201\_ г.

\_\_\_\_\_ (должность) \_\_\_\_\_ (подпись) \_\_\_\_\_ (Ф.И.О.)

М.П.

Номер заявки в IntraService – [ \_\_\_\_\_ ] (для внутреннего учета)

Начальник  
управления корпоративного бизнеса

Ю.В.Садаков

Управление корпоративного бизнеса