

ДОГОВОР на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2»

1. Термины и определения

В целях исполнения настоящего Договора на обслуживание клиента в системе дистанционного банковского обслуживания «iBank2» применяемые в нем термины и определения будут иметь следующие значения:

Банк – Общество с ограниченной ответственностью «Южный региональный банк» (ООО «ЮРБ»), имеющее Лицензию на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, выданную УФСБ России по Ростовской области.

Блокировочное слово – уникальное слово, определяемое Клиентом при осуществлении процедуры регистрации в системе «iBank2», которое используется Банком для голосовой идентификации Клиента.

Владелец ключа проверки электронной подписи – уполномоченное физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки ЭП и которое владеет соответствующим ключом электронной подписи, позволяющим ставить электронную подпись под электронными документами (подписывать электронные документы).

Договор – Договор на обслуживание клиента в системе дистанционного банковского обслуживания «iBank2», заключенный между Банком и Клиентом путем присоединения Клиента к настоящему Договору.

Дистанционное банковское обслуживание (ДБО) - комплекс услуг, предоставляемых Банком Клиенту в рамках системы «iBank2», пользователем которой является Клиент, включающий предоставление Банком Клиенту возможности передачи Банку Распоряжений с целью проведения расчетных операций по счету Клиента и предоставления информации о счете Клиента, а также взаимный обмен электронными документами, не являющимися электронными платежными документами, в том числе, предусмотренными валютным законодательством Российской Федерации.

Законодательство – действующее законодательство Российской Федерации, включая законы и подзаконные нормативные акты (в том числе нормативные акты Банка России и иных регулирующих и надзорных органов).

Заявление (Оферта) о присоединении - Заявление (Оферта) о присоединении к Договору на обслуживание клиента в системе дистанционного банковского обслуживания «iBank2».

Иные электронные документы – любой документ в электронном виде, кроме распоряжения, созданный Клиентом и Банком в системе «iBank2».

Клиент - юридическое лицо, индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством порядке частной практикой, находящееся на обслуживании в Банке на основании Договора банковского счета: плательщик, получатель и/или взыскатель средств, использующий электронный документооборот системы «iBank2» в соответствии с законодательством и настоящим Договором.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом электронной подписи Клиента, самостоятельно формируемая Клиентом с использованием средств системы «iBank2», и предназначенная для проверки Банком подлинности ЭП, созданной в электронном документе, сформированном Клиентом.

Ключ ЭП – уникальная последовательность символов, самостоятельно формируемая Клиентом с использованием средств системы «iBank2» и предназначенная для авторизации в системе «iBank2» и создания Клиентом электронной подписи в электронных документах.

Ключ ЭП действует на определенный момент времени, если:

- наступил момент времени начала действия ключа проверки ЭП Клиента;
- срок действия ключа проверки ЭП Клиента не истек;
- ключ проверки ЭП Клиента не аннулирован (отозван) и действие его не приостановлено.

Компрометация ключа ЭП - утрата доверия к тому, что используемый ключ ЭП (пара ключей ЭП) обеспечивает безопасность информации. К событиям, связанным с компрометацией ключа ЭП (пары ключей ЭП), относятся, в том числе, следующие события:

- утрата (в том числе хищение) носителя, на котором хранится ключ ЭП;
- утрата носителя, на котором хранится ключ ЭП, с последующим обнаружением;
- нарушение правил хранения ключа ЭП;
- несанкционированное копирование ключа ЭП (при такой возможности);

- случаи, когда нельзя достоверно установить, что произошло с ключом ЭП (в том числе случаи, когда ключ ЭП вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- возникновение подозрений на утечку информации или ее искажение в системе «iBank2»;
- доступ посторонних лиц к носителям ключевой информации;
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа третьих лиц к ключу ЭП.

Многофакторная аутентификация – дополнительная проверка подлинности Клиента, проводимая с использованием разового пароля, полученного посредством короткого сообщения (SMS).

Носитель ключевой информации (НКИ) – персональный аппаратный криптопровайдер (**USB-токен**) - устройство с неизвлекаемым хранением ключей ЭП, генерирующее ключи ЭП внутри себя, обеспечивающее их защищенное неизвлекаемое хранение в защищенной долговременной памяти и формирующее усиленную ЭП под электронными документами внутри устройства.

Операционное время - часть рабочего дня, отведенного для приема и обслуживания Клиентов в Банке и выполнения банковских операций текущим днем.

ОТР-токен - аппаратное устройство, позволяющее генерировать одноразовые пароли для дополнительной аутентификации Клиента при входе в систему «iBank2» и/или подтверждения Клиентом совершения расходных операций по счету.

Пакет электронных документов (пакет ЭД) - электронные документы, к которым присоединены один или несколько связанных между собой электронных документов, включая электронные образы документов (сканированные изображения документов, оформленных первоначально на бумажных носителях). При подписании пакета документов ЭП, каждый из присоединенных электронных документов, составляющих пакет, считается подписанным ЭП, которой подписан пакет документов.

Клиент самостоятельно определяет взаимосвязанность электронных документов при формировании пакета ЭД.

Перевод денежных средств – действия Банка, осуществляемые в пределах остатка денежных средств, находящихся на счете Клиента-плательщика, на основании переданного Клиентом с использованием системы «iBank2» распоряжения (или акцепта) на осуществление перевода в рамках применяемых форм безналичных расчетов, в целях предоставления денежных средств получателю средств.

Подтверждение подлинности ЭП в ЭД – процедура, дающая положительный результат проверки ЭП с использованием Ключа проверки ЭП принадлежности Сертификата ключа проверки ЭП в ЭД Владельцу ЭП. Результат проверки подтверждает отсутствие искажений в данном ЭД, подписанной данной ЭП.

Подразделения Банка – обособленные подразделения и внутренние структурные подразделения ООО «ЮРБ», которые наделены правом открытия, ведения и закрытия банковских счетов, а также правом заключения договоров на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».

Распоряжение - электронный платежный документ, созданный Клиентом в системе «iBank 2» и оформленный в соответствии с требованиями законодательства, а также договорами, заключенными между Банком и Клиентом.

Сервис «Мониторинг» - сервис, предоставляющий возможность Клиенту получать sms-уведомление и/или E-mail уведомление на зарегистрированный в системе «iBank2» номер телефона и/или адрес E-mail, содержащее сведения о входе Клиента в систему «iBank2», о движении денежных средств по счету (ам), открытому (ым) в Банке.

Сертификат ключа проверки ЭП Клиента – документ на бумажном носителе, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки электронной подписи.

Система «iBank2» - корпоративная информационная система дистанционного банковского обслуживания, совокупность программно-аппаратных средств, совместно эксплуатируемых Клиентом и Банком в соответствующих частях, с целью предоставления Клиенту услуг доступа к электронному документообороту системы «iBank2» в соответствии с настоящим Договором. Система «iBank2» является системой защищенного электронного документооборота, позволяющего Клиенту составлять, удостоверить и передавать в Банк распоряжения в целях осуществления переводов денежных средств, а также иных документов.

Средства ЭП - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций:

- создание электронной подписи;
- проверка электронной подписи;
- создание ключа электронной подписи и ключа проверки ЭП.

Стороны – Банк и Клиент.

Счет (счет Клиента) – банковский счет Клиента, открытый в Банке и зарегистрированный в системе «iBank2».

Тарифы Банка – Тарифы комиссионного вознаграждения ООО «ЮРБ» для юридических лиц и индивидуальных предпринимателей за предоставляемые услуги.

Удостоверяющий центр - Банк, обеспечивающий регистрацию и управление ключами проверки электронной подписи в системе «iBank2».

Усиленная электронная подпись – неквалифицированная электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа ЭП;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств ЭП.

Электронная подпись (ЭП) – реквизит электронного документа в системе «iBank2», предназначенный для защиты целостности данного электронного документа, полученный в результате криптографического преобразования информации с использованием ключа ЭП, позволяющего однозначно идентифицировать владельца данного ключа электронной подписи, а также установить отсутствие искажения информации в данном документе после его подписания. Электронный документ, подписанный ЭП в соответствии с настоящим Договором, считается подписанным усиленной неквалифицированной электронной подписью.

Электронный документ (ЭД) – совокупность символов, содержащая регламентируемую системой «iBank2» информацию для обмена между Клиентом и Банком. Неизменность и авторство данной информации удостоверены с использованием ЭП уполномоченного лица одной из Сторон. Электронные документы (распоряжения и иные электронные документы), подписанные электронной подписью, являются равнозначными соответствующим документам на бумажном носителе, оформленным в соответствии с законодательством и заверенным собственноручной подписью уполномоченным (ми) лицом (ами) и скрепленным оттиском печати Клиента (при наличии), согласно карточке с образцами подписей и оттиска печати Клиента, которые порождают аналогичные им права и обязанности участников взаимодействия электронного документооборота системы «iBank2».

Электронный документооборот (электронный документооборот системы «iBank2») - порядок обмена документами в электронном виде, осуществляемый в соответствии с настоящим Договором.

Электронное устройство (ЭУ) - персональный компьютер, ноутбук, планшетный компьютер и т.п., с помощью которого осуществляется работа в системе «iBank2».

2. Общие положения

2.1. Настоящий Договор устанавливает порядок взаимодействия между Сторонами при осуществлении электронного документооборота с использованием системы «iBank2» и определяет возникающие в связи с этим права, обязанности и ответственность Сторон.

2.2. Настоящий Договор является типовым формуляром Банка для всех Клиентов и договором присоединения в соответствии с законодательством.

2.3. Настоящий Договор распространяется на все счета Клиента, зарегистрированные в системе «iBank2».

2.4. Заключение настоящего Договора между Сторонами осуществляется путем присоединения Клиента к настоящему Договору и производится путем акцепта Банком (отметки Банка об акцепте) оферты Клиента (поданного в Банк Заявления (Оферты) о присоединении, составленного на бумажном носителе по форме Приложения № 1 к настоящему Договору).

В случае если Клиент уже осуществляет электронный документооборот с Банком посредством системы «iBank 2» на основании соответствующего договора, заключенного между Банком и Клиентом, Клиент вправе присоединиться к условиям настоящего Договора, предоставив в Банк Заявление (Оферту) о присоединении, составленное на бумажном носителе по форме Приложения № 1 к настоящему Договору.

При этом со дня акцепта Банком Заявления (Оферты) о присоединении, по форме Приложения № 1 к настоящему Договору, договор, применяемый до введения настоящего Договора, считается измененным и изложенным в редакции настоящего Договора.

2.5. Права и обязанности Сторон возникают с момента заключения настоящего Договора. Момент заключения настоящего Договора определяется и подтверждается отметкой Банка об акцепте Заявления (Оферты) о присоединении (Приложение № 1 к настоящему Договору). Отметка об акцепте проставляется Банком после проверки информации и документов, представленных Клиентом, их соответствия условиям работы в системе «iBank2». Пункты 9.4.-9.5. настоящего Договора вступают в силу с 01 января 2014 года.

2.6. Условием предоставления банковских услуг по переводу денежных средств с использованием

системы «iBank2» является наличие у Клиента счета в Банке.

3. Порядок подключения, получения доступа Клиента к системе «iBank2» и использования электронной подписи

3.1. Порядок подключения и получения доступа Клиента к системе «iBank2» основан на использовании электронной подписи в соответствии с законодательством, Руководством пользователя Системы «iBank2» для корпоративных клиентов и настоящим Договором.

3.2. В целях подключения Клиента к системе «iBank2» Клиенту следует:

3.2.1. Ознакомиться в обязательном порядке с размещенными на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.urb.ru/>) документами:

- Памяткой о рисках при работе в системе дистанционного банковского обслуживания «iBank2» (Приложение № 3 к настоящему Договору);
- Руководством пользователя Системы «iBank2» для корпоративных клиентов, содержащим условия использования системы «iBank2»;
- Требованиями по обеспечению информационной безопасности в системе «iBank2» (Приложение № 8 к настоящему Договору);
- Тарифами Банка.

3.2.2. Предоставить в Банк документы, необходимые для регистрации Клиента в системе «iBank2»:

- Заявление (Оферту) о присоединении по форме Приложения № 1 к настоящему Договору (в двух экземплярах);
- Заявление о выдаче USB-токена(ов)/ОТР-токена(ов) по форме Приложения № 2 к настоящему Договору;
- Акт приема-передачи USB-токена/ОТР-токена по форме Приложения № 5 к настоящему Договору (в двух экземплярах);
- Документы, необходимые для идентификации Клиента, представителей Клиента, выгодоприобретателей Клиента, бенефициарных владельцев Клиента по форме, в объеме и в порядке, установленном Банком (в одном экземпляре);
- Согласие владельца ключа ЭП на обработку персональных данных по форме Приложения № 4 к настоящему Договору (в одном экземпляре).

Документы предоставляются в Банк на бумажном носителе, подписанные собственноручной подписью уполномоченного лица и скрепленные оттиском печати Клиента (при наличии).

3.2.3. Оплатить комиссию в соответствии с Тарифами Банка.

3.2.4. Получить USB-токен/ОТР-токен. Факт приема - передачи USB-токена/ОТР-токена Клиентом подтверждается Актом приема-передачи USB-токена/ОТР-токена по форме Приложения № 5 к настоящему Договору.

3.2.5. Пройти процедуру предварительной регистрации в системе «iBank2». Указанная процедура осуществляется Клиентом самостоятельно на сервере системы «iBank2» в соответствии с требованиями настоящего Договора и Руководства пользователя Системы «iBank2» для корпоративных клиентов. В результате предварительной регистрации Клиента в системе «iBank2» формируются ключ ЭП и ключ проверки ЭП, а также сертификат ключа проверки электронной подписи, который необходимо распечатать в двух экземплярах.

3.2.6. Предоставить в Банк документы, необходимые для окончательной регистрации Клиента в системе «iBank2»:

- указанный в подпункте 3.2.5. настоящего Договора сертификат ключа проверки электронной подписи на бумажном носителе в 2 (Двух) экземплярах. Сертификат ключа проверки электронной подписи принимается Банком при наличии предоставленного в письменной форме согласия владельца ключа ЭП на обработку Банком персональных данных, указанных в Сертификате (Приложение № 4 к настоящему Договору);
- Акт выполненных работ по форме Приложения № 6 к настоящему Договору (в двух экземплярах).

Документы предоставляются в Банк на бумажном носителе, подписанные собственноручной подписью уполномоченного лица и скрепленные оттиском печати Клиента (при наличии).

3.3. После исполнения процедур, указанных в пункте 3.2. настоящего Договора, Клиенту следует получить свои экземпляры следующих документов:

- Заявление (Оферту) о присоединении по форме Приложения № 1 к настоящему Договору с отметкой Банка об акцепте;
- Сертификат ключа проверки ЭП;
- Акт приема-передачи USB-токена/ОТР-токена по форме Приложения № 5 к настоящему Договору;
- Акт выполненных работ по форме Приложения № 6 к настоящему Договору.

3.4. Банк предоставляет Клиенту возможность круглосуточного доступа в систему «iBank2» для формирования и передачи в Банк распоряжений и иных электронных документов, при этом:

- в качестве единой шкалы времени при работе в системе «iBank2» признается московское поясное время, контрольным является время системных часов серверов Банка системы «iBank2»;
- документы, поступившие в течение Операционного времени, Банк принимает к исполнению в тот же день, документы, поступившие после Операционного времени, – на следующий рабочий день;
- обработка электронных документов сотрудниками Банка осуществляется в соответствии с режимом работы Банка (Подразделений Банка), обслуживающих счет Клиента.

3.5. При осуществлении электронного документооборота Банком реализуются следующие принципы исполнения электронных документов, сформированных и переданных Клиентом в Банк вне Операционного времени:

- исполнение распоряжений Клиента осуществляется Банком не позднее операционного дня, следующего за днем поступления распоряжения в Банк, в соответствии с законодательством;
- исполнение иных электронных документов и сроки принятия по ним решений установлены соответствующими внутренними документами Банка.

3.6. Консультирование Клиента по вопросам электронного документооборота, является частью системы взаимодействия между Банком и Клиентом, согласно которому возможно обращение Клиента:

- за консультациями по вопросам, связанным с использованием системы «iBank2»;
- по вопросам заключения/изменения/расторжения настоящего Договора;
- по вопросам оформления распоряжений и иных электронных документов;
- по вопросам предоставления документов, связанных с проведением Клиентом валютных операций, подтверждающих (дополнительных) документов, предоставления консультаций по подписанию паспортов сделок, оформления документов унифицированной формы, исполнения запросов Клиента по валютному контролю.

Консультирование осуществляется по телефонам Банка в рабочее время Банка, в соответствии с установленным режимом работы Банка (Подразделений Банка).

4. Общие принципы предоставления услуг по осуществлению переводов денежных средств и электронного документооборота с использованием системы «iBank2»

4.1. Процедура создания и передачи Клиентом распоряжений и иных электронных документов с использованием системы «iBank2» предусматривает формирование этих документов на сервере Банка.

4.2. Перевод денежных средств с использованием системы «iBank2» может осуществляться в валюте Российской Федерации и в иностранной валюте.

4.3. Клиент имеет возможность предъявлять в Банк с использованием системы «iBank2» распоряжения для осуществления перевода денежных средств со своих счетов, открытых в Банке, в рамках следующих форм безналичных расчетов:

4.3.1. Расчеты платежными поручениями;

4.3.2. Расчеты по аккредитиву;

4.3.3. Расчеты инкассовыми поручениями;

4.3.4. Расчеты в форме перевода денежных средств по требованию получателя средств (расчеты платежными требованиями):

- Клиент, являясь получателем средств по платежному требованию, имеет возможность передавать распоряжения в Банк для предъявления Банком платежного требования плательщику;
- Клиент, являясь плательщиком по требованию получателя средств, имеет возможность предъявлять в Банк акцепт/заранее данный акцепт требования получателя средств о переводе денежных средств со счета Клиента в пользу получателя средств. Акцепт/заранее данный акцепт, предоставляется в Банк отдельным документом (Заявление об акцепте) с удостоверением ЭП Клиента;

4.3.5. Заявление на перевод в иностранной валюте;

4.3.6. Иными распоряжениями, формы которых утверждены Банком.

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

4.4.1. **Безотзывность перевода** денежных средств наступает с момента списания денежных средств со счета Клиента-плательщика.

4.4.2. **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 - при предоставлении Клиентом акцепта/заранее данного акцепта;
- при расчетах инкассовыми поручениями - при наличии 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.

4.4.3. **Окончателность перевода** денежных средств наступает:

- при переводе денежных средств на счет получателя, открытый в Банке, - в момент зачисления денежных средств на счет получателя;
- при переводе денежных средств на счета, открытые в иных кредитных организациях, - в момент зачисления денежных средств на счет банка-получателя денежных средств.

4.5. Распоряжения и иные электронные документы, передаваемые Клиентом в Банк с использованием системы «iBank2», должны быть оформлены в соответствии с требованиями законодательства и настоящего Договора.

4.6. Банк не имеет права вносить какие-либо изменения в распоряжения и иные электронные документы, принимаемые от Клиента по системе «iBank2».

4.7. Банк аннулирует ЭД в случае, если этот документ оформлен Клиентом с нарушением требований законодательства, и уведомляет об этом Клиента в соответствии с пунктом 4.14. настоящего Договора.

4.8. При необходимости дополнения/исправления указанных ранее сведений в ЭД, Клиент отзывает ЭД в соответствии с пунктом 4.13. настоящего Договора и предоставляет в Банк вновь сформированный ЭД.

4.9. Формирование Клиентом в системе «iBank2» и прием Банком к исполнению распоряжений Клиента и иных электронных документов, переданных в Банк с использованием системы «iBank2», осуществляется Банком при выполнении следующих процедур:

- удостоверение права распоряжения денежными средствами;
- контроль целостности распоряжений Клиента;
- контроль структуры и значений реквизитов;
- контроль достаточности денежных средств на счете Клиента.

Процедура контроля Банком распоряжений Клиента в иностранной валюте осуществляется в соответствии с пунктом 5.1. настоящих Правил.

4.10. **Удостоверение права распоряжения денежными средствами и контроль целостности** распоряжений и иных электронных документов, предоставляемых по системе «iBank2», Банк осуществляет посредством проверки ЭП и Многофакторной аутентификации в случае, если Клиент воспользовался своим правом на использование указанного сервиса.

Процедура проверки ЭП включает:

- проверку соответствия и подлинности ЭП;
- определение ключа проверки ЭП, соответствующего ключу ЭП, с использованием которого подписан ЭД;
- проверку целостности и неизменности ЭД (в том числе, реквизитов ЭД), созданного Клиентом и поступившего для исполнения в Банк.

В случае нарушения хотя бы одной процедуры проверки, проверяемый электронный документ отвергается системой «iBank2».

4.11. **Контроль структуры и значений реквизитов** распоряжений и иных электронных документов Клиента осуществляется посредством проверки соответствия реквизитов ЭД, сформированных Клиентом в системе «iBank2», требованиям законодательства.

4.12. **Контроль достаточности денежных средств на счете** Клиента осуществляется Банком при приеме распоряжения с учетом ограничений на распоряжение денежными средствами на счете, установленных законодательством, и с учетом поступления денежных средств на счет Клиента в течение текущего операционного дня.

4.12.1. Распоряжения Клиента исполняются Банком в порядке поступления в Банк (получения акцепта от Клиента) в пределах остатка денежных средств на счете Клиента.

4.12.2. При выявлении недостаточности денежных средств на счете Клиента, поступившие распоряжения Клиента не принимаются Банком к исполнению (отвергаются) за исключением:

- распоряжений, которые в соответствии с очередностью, установленной законодательством, помещаются в очередь не исполненных в срок распоряжений для дальнейшего осуществления контроля достаточности денежных средств на счете Клиента-плательщика (распоряжения о

переводе денежных средств в бюджеты бюджетной системы Российской Федерации и распоряжений этой же, либо предыдущей очередности списания денежных средств, установленной законодательством), а также распоряжений, принимаемых Банком к исполнению в соответствии с Договором банковского счета, заключенным с Клиентом.

4.13. Клиент вправе совершить отзыв распоряжения до наступления момента безотзывности перевода, предоставив в Банк электронное заявление об отзыве распоряжения по форме, предусмотренной в системе «iBank2», с указанием причины отзыва документа.

Заявление об отзыве служит основанием для возврата (аннулирования) Банком распоряжения.

4.14. Способом уведомления Клиента об аннулировании Банком распоряжений и иных электронных документов Клиента, Стороны признают присвоенный ЭД в системе «iBank2» **статус «Отвергнут»**. В системе «iBank2» Клиенту доступна информация, позволяющая идентифицировать аннулируемое распоряжение, дату его аннулирования и причину.

4.15. Способом уведомления Клиента о поступлении распоряжений и иных электронных документов Клиента на исполнение Стороны признают присвоенный ЭД в системе «iBank2» **статус «На обработке»**. Способом уведомления Клиента об исполнении Банком распоряжений и иных электронных документов, Стороны признают присвоенный ЭД в системе «iBank2» **статус «Исполнен»**. В системе «iBank2» Клиенту доступна информация, содержащая реквизиты Банка, вид операции, дату операции, сумму операции, идентификатор операции, статус ЭД.

4.15.1. Распоряжение Клиента может быть помещено Банком в очередь не исполненных в срок распоряжений по причине недостаточности денежных средств на счете Клиента-плательщика, либо в очередь распоряжений, ожидающих разрешения на проведение операций. Уведомление Клиента о помещении Банком поступившего распоряжения в очередь осуществляется Банком в электронном виде. Способом уведомления Клиента о постановке распоряжения в очередь Стороны признают **статус «На исполнении»**, присвоенный ЭД в системе «iBank2», с указанием даты и времени присвоения статуса.

4.15.2. Помещение Банком распоряжения Клиента в очередь распоряжений, не исполненных в срок, по причине недостаточности денежных средств на счете Клиента-плательщика, либо ожидающих разрешения на проведение операций, не является отрицательным результатом процедуры приема распоряжения к исполнению.

4.16. Дата отправления/принятия ЭД, переданного с использованием системы «iBank2», регистрируется системой и признается Сторонами фактической датой получения/отправки этого ЭД.

4.17. Данные по проведенным операциям текущего операционного дня по счету Клиента отражаются в выписке. Обновление данных в системе «iBank2» осуществляется непрерывно. Окончательное формирование выписки по счету Клиента осуществляется до 10 утра операционного дня, следующего за днем проведения операции по счету.

5. Особенности оказания банковских услуг с применением системы «iBank2» для осуществления валютных операций и электронного документооборота в целях валютного контроля

5.1. Процедура контроля Банком распоряжений Клиента в иностранной валюте: заявлений на перевод в иностранной валюте и распоряжений на списание с транзитного счета включает:

- контроль на соответствие законодательству;
- контроль структуры и значений реквизитов распоряжения;
- контроль на наличие полного, надлежаще оформленного комплекта документов и информации, связанных с проводимой валютной операцией, подтверждающих документов.

При приеме Банком к исполнению распоряжений Клиента в иностранной валюте и переводе денежных средств по счетам Клиента на основании поручений Клиента на покупку/продажу иностранной валюты Банк осуществляет процедуры, предусмотренные п. 4.9. настоящего Договора.

Списание денежных средств со счетов Клиента на основании вышеперечисленных распоряжений Клиента в иностранной валюте осуществляется Банком в безакцептном порядке в соответствии с договором банковского счета.

5.2. Иные электронные документы в целях валютного контроля, предоставляемые в Банк с использованием системы «iBank2»:

- поручения на покупку/продажу иностранной валюты;
- документы унифицированной формы - паспорт сделки по контракту, паспорт сделки по кредитному договору, справка о валютных операциях, справка о подтверждающих документах;
- иные документы и информация, включая электронные образы документов (сканированные изображения документов, оформленных первоначально на бумажных носителях),

составленные Клиентами в соответствии с законодательством, Договором банковского счета и настоящим Договором, имеют юридическую силу документов на бумажных носителях, оформленных в соответствии с

требованиями законодательства, подписанных соответствующим количеством подписей уполномоченных лиц и заверенных оттиском печати Клиента, и порождают аналогичные им права и обязанности Сторон.

Электронные документы, предоставляемые в Банк для осуществления валютных операций и электронного документооборота между Банком и Клиентом в целях валютного контроля, в том числе, взаимосвязанные документы, предоставляемые пакетом ЭД, присоединенным к сообщениям свободного формата, а также к документам унифицированной формы, подписываются ЭП.

При подписании ЭП Клиента сообщения свободного формата, а также указанных выше документов, являющихся документами унифицированной формы, каждый из присоединенных электронных документов (пакета присоединенных взаимосвязанных электронных документов), считается подписанным ЭП, которой подписано сообщение свободного формата или документы, являющиеся документами унифицированной формы.

5.3. Клиенту предоставляется право направлять в Банк подписанные ЭП документы унифицированной формы по валютным операциям, как сформированные в электронном виде с использованием соответствующих форм системы «iBank2» (включая приложения к указанным формам), так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажных носителях.

5.4. Сведения о текущем состоянии ЭД, формируемых в системе «iBank2» в целях валютного контроля, отображаются в системе «iBank2» автоматически путем изменения статуса ЭД в системе «iBank2».

5.4.1. Электронным документам, предоставляемым в Банк по системе «iBank2» в целях валютного контроля, присваиваются следующие статусы:

- «Доставлен» - получение Банком ЭД;
- «На обработке» - осуществление проверки ЭД сотрудником Банка, имеющим право совершать от имени Банка как агента валютного контроля действия по валютному контролю, предусмотренные законодательством (далее – Ответственный сотрудник Банка);
- «Исполнен» - прием и подписание ЭД со стороны Банка;
- «Отвергнут» - отказ в исполнении ЭД со стороны Банка (сопровождается комментариями о причинах возврата).

5.4.2. Дополнительную информацию (дополнительные ЭД) к вышеуказанным документам унифицированной формы, Клиент должен передавать в Банк одновременно с документами унифицированной формы.

5.4.3. При непринятии ЭД Банком, ЭД переводится в статус «Отвергнут», с обязательным указанием причины отказа в принятии ЭД и отображением в системе «iBank2» даты присвоения данного статуса.

5.5. Клиент должен контролировать получение информации о ходе исполнения Банком ЭД, указанных в пункте 5.4. настоящего Договора. В случае нарушения электронного документооборота, несвоевременного получения информации, Клиент обязан немедленно уведомлять об этом сотрудников Банка по телефону, с последующим подтверждением в письменной форме не позднее следующего операционного дня.

5.6. Датой предоставления Клиентом в Банк ЭД для целей валютного контроля является дата их получения Банком, зарегистрированная в системе «iBank2» при их отправке. Дата предоставления ЭД в Банк может отличаться от даты принятия к обработке таких ЭД Банком.

5.7. Датой получения Клиентом от Банка ЭД валютного контроля в системе «iBank2» является дата их отправки Банком, или изменения статуса ЭД, зафиксированная в системе «iBank2».

5.8. Течение срока проверки Банком ЭД, представленных Клиентом в целях осуществления валютного контроля, начинается с момента предоставления документов в Банк с даты, обозначенной в системе «iBank2» статусом «Доставлен». Сроки проверки Банком документов установлены в соответствии с законодательством.

5.9. Иные ЭД для целей осуществления расчетов в иностранной валюте и целей валютного контроля, подписанные ЭП, а именно: договоры, контракты и соглашения, акты, счета, счета фактуры, документы к любым изменениям валютных контрактов и т.п. могут передаваться в Банк в электронном виде с применением электронных образов (сканированные изображения документов, оформленных первоначально на бумажных носителях).

5.9.1. Предоставляемые Клиентом документы с применением электронных образов должны быть доступны для чтения без использования специальных устройств. Банк принимает к исполнению документы только при надлежащем качестве предоставляемых в Банк копий оригинальных документов (отражение без искажений всех элементов документа) и доступности для прочтения текста в предоставляемых документах с применением электронных образов, присоединенных к сообщениям свободного формата, а также к документам унифицированных форм.

6. Права и обязанности Сторон

6.1. Банк обязан:

6.1.1. Обеспечивать функциональность электронного документооборота в системе «iBank2», применять меры защиты передаваемой информации с использованием средств криптографической защиты информации (СКЗИ) в соответствии с требованиями законодательства в области защиты информации.

6.1.2. Регистрировать в течение 3 (Трех) рабочих дней новый ключ ЭП Клиента на основании предоставленного Сертификата ключа проверки ЭП.

6.1.3. В случае замены ключа проверки ЭП, немедленно блокировать действующий до этого момента ключ проверки ЭП.

6.1.4. В случае устного обращения Клиента с применением голосовой идентификации «Блокировочное слово» или получением Банком письменного уведомления в произвольной форме, заверенного подписью уполномоченного лица и оттиском печати Клиента (при наличии), блокировать существующий ключ ЭП.

6.1.5. Информировать Клиента о входах в систему «iBank2» и совершении операций по переводу денежных средств с использованием системы «iBank2» путем направления Клиенту SMS-уведомлений и/или E-mail-уведомлений в соответствии с Порядком уведомления Клиента о совершении операций в системе «iBank2» (Приложение № 9 к настоящему Договору).

6.1.6. Обеспечить возможность направления Клиентом в Банк уведомления о компрометации ключей ЭП (в том числе, об утрате НКИ) и (или) их использовании без согласия Клиента.

6.1.7. Возместить Клиенту сумму операции, совершенной без согласия Клиента, после получения Банком письменного уведомления Клиента об утрате НКИ и (или) его использования без согласия Клиента.

6.1.8. Фиксировать направленные Клиенту и полученные от Клиента уведомления, а также хранить соответствующую информацию не менее 3 (Трех) лет.

6.1.9. Консультировать Клиента по вопросам эксплуатации системы «iBank2» и ее настройке, в том числе, размещая актуальную информацию на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.urb.ru/>).

6.1.10. Предоставлять Клиенту документы и информацию, связанные с использованием Клиентом системы «iBank2», в течение 5 (Пяти) рабочих дней с момента получения письменного требования Клиента.

6.1.11. Рассматривать заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом системы «iBank2», а также предоставить Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в течение 15 (пятнадцати) рабочих дней со дня получения таких заявлений.

6.2. Банк имеет право:

6.2.1. Блокировать действующий ключ ЭП Клиента, и требовать от Клиента смены пары ключей ЭП Клиента:

- в случае возникновения подозрений в их компрометации;
- по истечении срока действия полномочий владельца ключа проверки ЭП, устанавливаемого Банком на основании учредительных документов, распорядительного акта Клиента либо выданной им доверенности;
- в иных случаях.

6.2.2. Блокировать действующий ключ ЭП Клиента в случае не выполнения Клиентом условий раздела 7 настоящего Договора, не позднее дня, следующего за днем исполнения обязательств Клиента по уплате ежемесячной абонентской оплаты. При погашении задолженности и предоставлении Клиентом в Банк заявления в произвольной форме о возобновлении работы в системе «iBank2», работа Клиента в системе «iBank2» возобновляется.

6.2.3. В случае возникновения у Банка сомнений в правомерности осуществления Клиентом электронного документооборота и/или в случае выявления в деятельности Клиента операций, в отношении которых возникают подозрения, что они осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, не принимать к исполнению электронные документы и требовать от Клиента оформления документа на бумажном носителе, предварительно уведомив Клиента в произвольной форме по системе «iBank2» не позднее операционного дня, следующего за днем получения соответствующего ЭД. Датой уведомления считается дата подписания сообщения ЭП сотрудником Банка.

6.2.4. Требовать от Клиента предоставления документов и сведений, необходимых в соответствии с требованиями законодательства в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

6.2.5. В случае не предоставления вышеуказанных документов отказать Клиенту в приеме от него распоряжений, подписанных ЭП Клиента, и принимать от Клиента только надлежащим образом оформленные расчетные документы на бумажном носителе.

6.2.6. Отказать в исполнении ЭД Клиента, составляющих пакет ЭД, если они, по мнению Банка, не являются взаимосвязанными.

6.2.7. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих приему и передаче ЭД через систему «iBank2», в одностороннем порядке приостановить до момента устранения неисправности электронный документооборот через систему «iBank2». В этом случае документооборот между Сторонами осуществляется на бумажных носителях.

6.2.8. Не исполнять ЭД Клиента, если они не соответствуют требованиям законодательства к их оформлению, не содержащих ЭП и иных необходимых реквизитов.

6.2.8.1. Не исполнять ЭД Клиента, если они не прошли дополнительную проверку подлинности Клиента, проводимую с использованием разового пароля, полученного посредством короткого сообщения (SMS), в случае, если Клиент воспользовался своим правом на использование сервиса Многофакторной аутентификации (некорректно/неверно/несвоевременно введен пароль, полученный посредством короткого сообщения (SMS)).

6.2.9. Отказать в доступе Клиента в систему «iBank2» в случае неподтверждения Клиентом входа в систему одноразовым паролем, полученным посредством короткого сообщения (SMS), в случае, если Клиент воспользовался своим правом на использование сервиса Многофакторной аутентификации (некорректно/неверно/несвоевременно введен пароль, полученный посредством короткого сообщения (SMS)).

6.2.10. Осуществлять блокировку работы Клиента в системе «iBank2» на основании полученного от Клиента уведомления или по инициативе Банка при нарушении Клиентом порядка использования системы «iBank2», в том числе, условий п. 6.3.16. настоящего Договора, несоблюдении им требований Банка по использованию криптографических и иных средств защиты информации.

6.2.11. Вносить в одностороннем порядке изменения в условия настоящего Договора и Тарифы Банка.

6.3. Клиент обязан:

6.3.1. Организовать рабочее место для работы в системе «iBank2» в соответствии с Требованиями по обеспечению информационной безопасности (Приложение № 8 к настоящему Договору).

6.3.2. Использовать ЭУ, с помощью которого осуществляется работа в системе «iBank2», исключительно в целях, предусмотренных настоящим Договором, и в соответствии с Руководством пользователя Системы «iBank2» для корпоративных клиентов.

6.3.3. Принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства ЭУ Клиента, изменение их состава, появление на ЭУ компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения системы «iBank2», ЭД, либо на перехват паролей, ключей ЭП и другой конфиденциальной информации.

6.3.4. Реализовать комплекс мер и средств защиты информации при использовании сети Интернет, обеспечивающий защиту данных от несанкционированного доступа по сети.

6.3.5. Использовать антивирусное программное обеспечение и своевременно осуществлять его обновление, а также обновления ПО «Java», операционной системы и Web-браузеров.

6.3.6. Организовать порядок хранения и использования носителей ключевой информации, который должен исключать возможность несанкционированного доступа к ним.

6.3.7. Не допускать:

- передачу носителей ключевой информации посторонним лицам;
- оставление носителей ключевой информации без присмотра;
- несанкционированное копирование информации с носителей ключевой информации с ключом ЭП;
- вывода содержимого файла ключей ЭП на дисплей (монитор) персонального компьютера или распечатывание его на бумажном носителе;
- подключение носителей ключевой информации к ЭУ иным способом и в режимах, не предусмотренных функционированием системы «iBank2»;
- записи на носитель ключевой информации посторонней информации.

6.3.8. Переоформить ЭП при изменении реквизитов, наименования организации, смене уполномоченных лиц и иных данных Клиента, в течение 3 (Трех) рабочих дней с даты таких изменений. В противном случае всю ответственность за правильность оформления электронных документов и перевода денежных средств с помощью системы «iBank2» несет Клиент.

6.3.9. В случае утраты НКИ и (или) его использования без согласия Клиента незамедлительно после обнаружения факта утраты НКИ и (или) его использования без согласия Клиента уведомить Банк одним из следующих способов:

- посредством телефонной связи, используя для идентификации Клиента «Блокировочное слово» в целях приостановления Банком использования Клиентом системы «iBank2»;
- путем направления соответствующего сообщения по адресу электронной почты Банка: info@urb.ru;

- с помощью факсимильной связи

с обязательным последующим направлением в Банк не позднее следующего операционного дня письменного уведомления в произвольной форме, заверенного подписью уполномоченного лица и оттиском печати Клиента (при наличии).

6.3.10. Незамедлительно информировать сотрудников Банка по телефону обо всех случаях компрометации ключа ЭП, повреждениях технических и программных средств ЭУ, а также о других обстоятельствах, которые делают возможным создание электронных документов и их передачу в Банк лицами, не имеющими соответствующих полномочий.

6.3.11. В случаях выявления хищения денежных средств в системе «iBank2» предпринять действия в соответствии с Порядком действий Сторон в случае выявления хищения денежных средств в системе «iBank2» (Приложение № 11 к настоящему Договору)

6.3.12. Не реже одного раза в неделю, а при наличии ежедневных платежей не реже одного раза в день, принимать в системе «iBank2» информацию (выписки по счетам, сообщения свободного формата, иные документы), переданную Банком, и производить сверку платежей.

6.3.13. Соблюдать согласованный Сторонами порядок подготовки и заполнения электронных документов.

6.3.14. По первому требованию Банка, но не позднее 2 (Двух) рабочих дней с даты получения такого требования, предоставить копии отправленных или полученных электронных документов на бумажном носителе, заверенные собственноручной подписью уполномоченного лица и печатью Клиента (при наличии).

6.3.15. Предоставлять по запросу Банка документы и сведения, необходимые в соответствии с требованиями нормативных документов в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

6.3.16. Предоставлять Банку достоверную информацию для связи с Клиентом, а в случае ее изменения своевременно предоставить обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений, предусмотренных п. 6.1.5. настоящего Договора, считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом.

6.3.17. Руководствоваться актуальной информацией по работе в системе «iBank2», размещенной на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.urb.ru/>).

6.3.18. Периодически знакомиться с размещенными на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или на сайте Банка <http://www.urb.ru/>) документами и информацией.

6.3.19. В порядке, установленном настоящим Договором, оплачивать оказываемые Банком услуги. Арест денежных средств на счете, приостановление операций по счету налоговыми и другими органами, не освобождает Клиента от обязанностей по оплате услуг Банка по обслуживанию системы «iBank2».

6.3.20. Подтверждать остатки по счету (ам) в соответствии с Договором банковского счета.

6.4. Клиент имеет право:

6.4.1. Досрочно прекратить действие своего действующего ключа ЭП и потребовать от Банка заблокировать соответствующий ему ключ проверки ЭП Клиента, обратившись по телефону и используя для голосовой идентификации «Блокировочное слово» Клиента (с последующим подтверждением в письменной форме не позднее следующего операционного дня).

6.4.2. Обратиться в Банк с требованием приостановить предоставление Банком услуг с использованием дистанционного банковского обслуживания в системе «iBank2».

Приостановка предоставления Банком услуг с использованием дистанционного банковского обслуживания в системе «iBank2» осуществляется по письменному заявлению Клиента в произвольной форме.

6.4.3. Отозвать свой электронный документ в порядке, предусмотренном настоящим Договором.

6.4.4. Предоставлять документы и информацию в Банк на бумажном носителе в случае невозможности использования системы «iBank2».

6.4.5. Пользоваться при работе в системе «iBank 2» сервисом «Мониторинг», предоставляемым в порядке и на условиях, определенных в Порядке уведомления Клиента о совершении операций в системе «iBank2» (Приложение № 9 к настоящему Договору).

6.4.6. Пользоваться при работе в системе «iBank 2» сервисом Многофакторной аутентификации, предоставляемым на основании заявления Клиента об использовании указанного сервиса (Приложение № 2.1 к настоящему Договору).

7. Порядок оплаты

7.1. За осуществление абонентского обслуживания по системе «iBank2» Клиента Банк взимает плату в соответствии с Тарифами Банка, с которыми Клиент ознакомлен и согласен.

7.2. Клиент предоставляет Банку право на безакцептное списание комиссионного вознаграждения Банка за обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» в соответствии с Тарифами Банка со счета Клиента.

8. Конфиденциальность

8.1. Стороны обязуются сохранять конфиденциальность относительно содержания настоящего Договора, а также любой информации и данных, предоставляемых каждой из Сторон в связи с исполнением настоящего Договора, не раскрывать и не разглашать третьим лицам в целом или частично факты и информацию без получения предварительного письменного согласия другой Стороны в период действия настоящего Договора и в течение 5 (Пяти) лет с даты его прекращения, за исключением случаев, установленных законодательством. Обязательства конфиденциальности, возложенные на Стороны, не распространяются на общедоступную информацию.

9. Ответственность Сторон

9.1. За неисполнение и/или ненадлежащее исполнение обязательств, предусмотренных настоящим Договором, Стороны несут ответственность в соответствии с законодательством.

9.2. Стороны несут ответственность за содержание ЭД, подписанных ЭП их уполномоченных лиц, и не отвечают за правильность заполнения и оформления ЭД другой Стороной.

9.3. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств, предусмотренных настоящим Договором, если такое неисполнение явилось следствием обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, изменения законодательства и иных обстоятельств, не зависящих от волеизъявления Сторон, возникших после заключения настоящего Договора, наступление которых Сторона не могла ни предвидеть, ни предотвратить доступными ей мерами, если такие обстоятельства непосредственно влияют на возможность исполнения Сторонами обязательств по настоящему Договору. При этом срок исполнения обязательств отодвигается соразмерно времени, в течение которого действовали такие обстоятельства.

9.4. В случае неисполнения Банком обязанности по информированию Клиента о совершенной операции в соответствии с п. 6.1.5. настоящего Договора, Банк обязан возместить Клиенту сумму операции, о которой Клиент не был проинформирован и которая была совершена без согласия Клиента.

9.5. При надлежащем исполнении Банком обязанности по информированию Клиента о совершенной операции в соответствии с п. 6.1.5. настоящего Договора и в случае неисполнения Клиентом обязанности, предусмотренной п. 6.3.9. настоящего Договора, Банк не возмещает Клиенту сумму операции по счету Клиента, совершенной без согласия Клиента.

9.6. Ответственность за действия сотрудников Клиента, имеющих доступ к системе «iBank2», электронным документам и ЭП, Клиент несет самостоятельно.

9.7. **Банк не несет ответственности за:**

- сбои в работе системы «iBank2», произошедшие не по вине Банка и повлекшие для Клиента невозможность передачи электронных документов;
- состояние и неработоспособность технических и программных средств Клиента, правильность установки и работы системного и прикладного программного обеспечения, настроек политик безопасности программного обеспечения и их антивирусной защиты, повлекшие за собой невозможность доступа Клиента в систему «iBank2» и возникшие в результате задержки в осуществлении платежей/распоряжений Клиента;
- несвоевременную доставку или наличие искажений в сообщениях Клиента, произошедших по техническим причинам из-за неполадок, сбоев в общедоступных коммуникационных сетях;
- ущерб, возникший вследствие разглашения уполномоченными лицами Клиента собственного ключа ЭП, его утраты или его передачи в независимости от причин неуполномоченным лицам;
- действия или бездействие Клиента или третьего лица (в том числе оператора связи), повлекшее неполучение Клиентом данных, переданных Банком через систему «iBank2», а также посредством сервиса «Мониторинг», в том числе в результате сбоев в работе организаций, предоставляющих услуги мобильной, телефонной или почтовой связи, утери телефона Клиентом, несвоевременного сообщения Клиентом сведений об изменении реквизитов для связи с Клиентом и т.д.

10. Порядок разрешения спора

10.1. Все споры и разногласия, возникшие в результате исполнения условий настоящего Договора, разрешаются путем переговоров.

10.2. В случае возникновения спорных ситуаций между Клиентом и Банком при использовании системы «iBank2» Стороны обязуются участвовать в рассмотрении споров в соответствии с Положением о порядке

проведения технической экспертизы при возникновении спорных ситуаций (Приложение № 7 к настоящему Договору), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению спорной ситуации.

10.3. Споры и разногласия, которые не могут быть урегулированы путем взаимных переговоров Сторон, подлежат рассмотрению в Арбитражном суде Ростовской области.

11. Порядок изменения, дополнения и расторжения Договора

11.1. Внесение изменений и/или дополнений в настоящий Договор и/или Тарифы Банка, в том числе утверждение Банком новой редакции настоящего Договора, производится по инициативе Банка в порядке, предусмотренном настоящим разделом.

11.2. Типовая форма Заявления (Оферты) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» определяется Банком в одностороннем порядке. Типовая форма Заявления (Оферты) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» доводится до сведения лиц, намеревающихся заключить настоящий Договор, путем размещения его на общедоступных ресурсах Банка (информационных стендах в операционных залах и/или сайте Банка <http://www.urb.ru/>).

11.3. 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 в действие новой редакции настоящего Договора, и/или Тарифов Банка за 10 (Десять) рабочих дней до даты введения в действие новых Тарифов, путем размещения указанных документов на общедоступных ресурсах Банка (информационных стендах в операционных залах Банка/Подразделений Банка, на сайте Банка в сети Интернет <http://www.urb.ru/>) и путем отправки информационного сообщения по системе «iBank2».

11.4. В случае несогласия Клиента с изменениями и/или дополнениями, внесенными Банком в настоящий Договор и/или Тарифы Банка, Клиент имеет право расторгнуть настоящий Договор в порядке, предусмотренном пунктом 11.6. настоящего Договора.

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

11.6. Банк и Клиент вправе отказаться от исполнения настоящего Договора в одностороннем, внесудебном порядке, при условии письменного уведомления другой Стороны не позднее, чем за 1 (Один) месяц до даты расторжения и урегулировании всех финансовых обязательств по настоящему Договору.

12. Заключительные положения

12.1. Клиент подтверждает, что им будет обеспечено предоставление физическими лицами, чьи персональные данные содержатся в предоставляемых Клиентом Банку документах, согласия на обработку (включая автоматизированную обработку) указанных персональных данных в соответствии с требованиями законодательства, по форме, установленной Банком.

12.2. Невозможность выполнения каких-либо условий Договора в результате изменений законодательства, произошедших после его заключения, не влияет на обязательность исполнения Сторонами остальных условий Договора.

12.3. Настоящий Договор содержит следующие Приложения, являющиеся его неотъемлемой частью:

- Приложение № 1 – Заявление (Оферта) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2»;
- Приложение № 2 – Заявление о выдаче USB-токена(ов)/ОТР-токена(ов);
- Приложение № 2.1. – Заявление об использовании (подключении) сервиса Многофакторной аутентификации
- Приложение № 3 – Памятка о рисках при работе в системе дистанционного банковского обслуживания «iBank2»;
- Приложение № 4 – Согласие на обработку персональных данных;
- Приложение № 5 – Акт приема-передачи USB-токена/ОТР-токена;
- Приложение № 6 – Акт выполненных работ;
- Приложение № 7 – Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций;
- Приложение № 8 – Требования по обеспечению информационной безопасности при работе в системе «iBank2»;
- Приложение № 9 – Порядок уведомления Клиента о совершении операций в системе «iBank2»;

- Приложение № 10 – Требования к аппаратно-программному обеспечению Клиента для работы в системе «iBank2»;
- Приложение № 11 – Порядок действий Сторон в случае выявления хищения денежных средств в системе «iBank2».

в ООО «ЮРБ»

**Заявление (Оферта) № _____
о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского
обслуживания «iBank2»**

Полное наименование Клиента:	
Сокращенное наименование Клиента:	
ИНН/КИО:	
ОГРН/ОГРНИП:	
Адрес места нахождения:	
Адрес фактического местонахождения:	
Контактная информация:	

1. Настоящим вышеуказанный Клиент заявляет о присоединении к действующей в ООО «ЮРБ» редакции Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» и подтверждает, что все положения (условия) действующей в ООО «ЮРБ» редакции Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» ему известны и разъяснены в полном объеме (включая все приложения и Тарифы Банка).

2. Настоящим вышеуказанный Клиент просит начать предоставление услуг в рамках Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» и зарегистрировать в системе «iBank2» следующий(е) счет(а), открытый(е) в ООО «ЮРБ»:

№п/п	№№ банковских счетов
1.	
2.	
3.	

3. Информация об уполномоченных лицах Клиента:

	№ п/п	Фамилия, Имя, Отчество	Должность	Паспортные данные
С правом подписи и отправки документов *	1.			
	2.			
	3.			
Без права подписи и отправки документов **	1.			
	2.			

* - указываются данные уполномоченных представителей Клиента, включенных в карточку с образцами подписей и оттиска печати Клиента и имеющих право подписи, отправки и отзыва электронных документов;

** - указываются данные об уполномоченных представителях Клиента, не имеющих права подписи, отправки и отзыва электронных документов.

4. Контактная информация для информирования Клиента об операциях, совершенных в системе «iBank2»:

ФИО ответственного лица	№ мобильного телефона ответственного лица (для приема SMS-уведомлений)	Адрес электронной почты ответственного лица (для приема E-Mail уведомлений)
1	2	3

В случае, если Клиент отказывается от получения уведомлений Банка о совершении операций по счетам в системе «iBank2» в соответствии со Статьей 9 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее ФЗ № 161-ФЗ), в столбцах 2 и 3 таблицы Уполномоченным лицом Клиента делается запись: «Отказываюсь от получения SMS-уведомлений/E-Mail уведомлений.».

В случае отказа Клиента от предоставления контактной информации для информирования Клиента об операциях, совершенных в системе «iBank2», обязанность Клиента о предоставлении

Банку достоверной информации в соответствии с п. 13 статьи 5 ФЗ № 161-ФЗ считается невыполненной, а обязанность Банка по информированию Клиента в соответствии с п. 4 статьи 9 ФЗ № 161-ФЗ считается исполненной.

5. Информация о сотрудниках Клиента, ответственных за обеспечение информационной безопасности.

ФИО ответственного лица	Должность ответственного лица	№ телефона ответственного лица	Адрес электронной почты ответственного лица
1	2	3	4

6. Перечень IP-адресов, разрешенных для работы в системе «iBank2».

Настоящим вышеуказанный Клиент уведомляет Банк о том, что работа в системе «iBank2» разрешена (выбрать нужное):

Только с указанных IP-адресов

Только с указанных IP-сетей

Без ограничения IP-адресов.

7. Настоящим вышеуказанный Клиент дает согласие на безакцептное списание комиссионного вознаграждения Банка за обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» в соответствии с Тарифами Банка со счетов Клиента.

8. С подписанием настоящего Заявления (Оферты) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания iBank2 вышеуказанный Клиент соглашается с тем, что ранее заключенный Договор на обслуживание Клиента в системе дистанционного банковского обслуживания iBank2 № _____ от «___» _____ 20__ г., заключенный между ним и ООО «ЮРБ», считается измененным и изложенным в редакции настоящего Договора на обслуживание Клиента в системе дистанционного банковского обслуживания iBank2. ***

Клиент:

_____ (должность уполномоченного лица) _____ (подпись) _____ (ФИО)
М.П.

Отметка Банка:

Настоящее Заявление (Оферта) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» акцептовано Банком «___» _____ 20__ года

_____ (должность уполномоченного лица) _____ (подпись) _____ (ФИО)
М.П.

Уважаемые Клиенты, обращаем Ваше внимание!

Консультирование по вопросам электронного документооборота в системе « iBank2» осуществляется по следующим телефонам:

(499) 918-71-92, (863) 250-11-46 (доб. 1123, 1124, 1131, 2132), (863) 250-11-47 - по вопросам подключения и использования системы «iBank2»;

(863) 250-11-48, доб. 1122, 1128 - по вопросам заключения/изменения/расторжения настоящего Договора;

(863) 250-11-48, доб. 1112, 1117, 1118 - по вопросам оформления электронных документов;

(863) 250-11-48, доб. 1130 - по вопросам предоставления документов, связанных с проведением Клиентом валютных операций, подтверждающих (дополнительных) документов, предоставления консультаций по подписанию паспортов сделок, оформления документов унифицированной формы учета, исполнения запросов Клиента по валютному контролю.

Консультирование осуществляется по телефонам Банка в рабочее время Банка, в соответствии с установленным режимом работы Банка (Подразделений Банка).

*** - Заполняется при наличии у Клиента ранее заключенного(ых) Договора(ов) на обслуживание по системе «iBank2».

**Заявление
о выдаче USB-токена(ов)/ОТР-токена(ов)**

1. Настоящим _____ (далее –
Клиент)

(наименование организации)

просит на основании Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» выдать для работы в системе «iBank2»:

USB-токен в количестве _____ шт.

ОТР-токен в количестве _____ шт.

Вышеуказанные USB-токен(ы)/ОТР-токен(ы) прошу выдать на руки и наделяю правом подписи Акта приема-передачи USB-токена/ОТР-токена следующее лицо:

Фамилия, Имя, Отчество	Должность	Паспортные данные

Клиент:

(должность уполномоченного лица)

(подпись)

М.П.

(_____)
(ФИО)

**Заявление
об использовании (подключении) сервиса Многофакторной аутентификации**

Настоящим _____ (далее – Клиент)
(наименование организации)

просит на основании Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2» подключить сервис Многофакторной аутентификации для работы в системе «iBank2»:

ФИО уполномоченного лица	№ мобильного телефона уполномоченного лица (для получения одноразовых паролей контроля входа в систему «iBank2» и подтверждения произведенных платежей)

Клиент:

(должность уполномоченного лица)

(подпись)
М.П.

(_____)
(ФИО)

ПАМЯТКА

о рисках при работе в системе дистанционного банковского обслуживания «iBank2»

Настоящим Общество с ограниченной ответственностью «Южный региональный банк» (ООО «ЮРБ») информирует Вас о повышенном риске при использовании системы дистанционного банковского обслуживания (далее – ДБО) и о возможных рисках несанкционированного доступа к персональной информации пользователей систем ДБО: логинов, паролей, ключей электронных подписей.

Анализ выявленных случаев хищения денежных средств с расчетных счетов Клиентов, проведенный Центральным банком Российской Федерации совместно с уполномоченными органами, показал, что хищения осуществляются:

- ответственными сотрудниками Клиентов, имевшими доступ к носителям ключевой информации (далее - НКИ) и ключам ЭП. Как правило, это уволенные руководители, бухгалтеры и их заместители, а также совладельцы организаций;
- штатными ИТ-сотрудниками Клиентов, имевшими технический доступ к НКИ, а также доступ к электронным устройствам Клиента (персональные компьютеры, ноутбуки, планшетные компьютеры и т.п.), с помощью которого осуществляется работа в системе дистанционного банковского обслуживания;
- нештатными, приходящими по вызову ИТ-специалистами, обслуживающими электронные устройства Клиентов, с которых осуществлялась работа в системе дистанционного банковского обслуживания (далее – ЭУ), в том числе специалистами, осуществляющими профилактику и подключение к сети Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого программного обеспечения;
- злоумышленниками путем заражения через сеть Интернет ЭУ Клиентов вредоносными программами. Используя уязвимости системного и прикладного программного обеспечения, ЭУ Клиентов заражаются троянскими программами с последующим дистанционным похищением ключей ЭП Клиента и паролей. Также с помощью троянских программ злоумышленники могут получить удаленный доступ к ЭУ Клиента и соответственно к ключам ЭП Клиента.

Обращаем Ваше внимание на то, что в ряде кредитных организаций были зафиксированы попытки хищения денежных средств у Клиентов, использовавших устройства с неизвлекаемыми ключами электронной подписи - USB - токенами. Во всех выявленных случаях злоумышленники пользовались халатностью Клиентов, оставляющих USB-токен постоянно и бесконтрольно подключенным к ЭУ, имеющему доступ в сеть Интернет. С помощью вредоносных программ со встроенным механизмом удаленного управления (RAdmin, TeamViewer, VNC и др.) злоумышленники подключались к консоли инфицированного ЭУ Клиента, запускали Web-браузер и подключались к portalу кредитной организации. Далее с использованием ранее перехваченного пароля доступа и постоянно подключенного USB-токена злоумышленники от имени Клиента заходили в систему ДБО, создавали расчетные документы, подписывали их и отправляли в кредитную организацию.

Одновременно были зафиксированы попытки хищения денежных средств со счетов Клиентов с использованием вредоносных программ, обеспечивающих дистанционный доступ к USB-портам ЭУ Клиента. При этом вход в систему ДБО осуществлялся с компьютера злоумышленника, а работа с USB - токеном, подключенным к ЭУ Клиента, происходила дистанционно. Для преодоления механизма контроля доступа Клиента в систему ДБО с заданных IP-адресов вредоносная программа осуществляла туннелирование TCP-трафика с компьютера злоумышленника до ЭУ Клиента внутри XMPP-трафика (Jabber и т.п.), производила трансляцию IP-адресов (NAT) и направляла TCP-трафик злоумышленника от Клиента в кредитную организацию.

Кроме вышеперечисленных сценариев хищения денежных средств при использовании системы ДБО в российских банках были зарегистрированы попытки хищения денежных средств Клиентов с использованием новой разновидности вредоносной программы, нативная компонента которой устанавливалась на ЭУ Клиента, используя критические уязвимости в старых версиях Java-машин (JVM). Вредоносная программа не только предоставляла возможность дистанционного управления ЭУ клиента, но и подменяла вызовы JVM для сокрытия мошеннических действий.

Расчетный документ создавался от имени Клиента, подписывался и отправлялся в кредитную организацию непосредственно с инфицированного ЭУ Клиента. При этом все мошеннические действия и их результаты оставались скрытыми от Клиента:

- При работе на инфицированном ЭУ Клиента мошеннический платеж не отображался в списке расчетных документов. При работе с обычного ЭУ мошеннический платеж отображался.
- При работе на инфицированном ЭУ Клиента операция списания денежных средств не отображалась в выписке из счета Клиента. При работе с обычного ЭУ операция отображалась.
- При работе на инфицированном ЭУ Клиента остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного ЭУ отображался реальный остаток.

В результате таких действий хищение денежных средств могло длительное время оставаться скрытым от сотрудников Клиента.

Председателю правления Общества с ограниченной ответственностью «Южный региональный банк» (ООО «ЮРБ»), расположенного по адресу: Российская Федерация, Ростовская область, 344006, г. Ростов-на-Дону, ул. Пушкинская, д. 144а,

от _____
(ФИО)

СОГЛАСИЕ на обработку персональных данных

Я, _____,
(ФИО)

зарегистрированный (ная) по адресу г. _____, ул. _____, д. _____, кв. _____,
паспорт _____, выдан _____, _____ 20____
(кем выдан) (дата)

свободно, своей волей и в своем интересе даю согласие Обществу с ограниченной ответственностью «Южный региональный банк» (далее – ООО «ЮРБ») на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

- фамилия, имя, отчество (ФИО);
- реквизиты документа, удостоверяющего личность: серия, номер, дата выдачи, наименование выдавшего органа, код подразделения;
- дата и место рождения;
- гражданство;
- адрес регистрации (места жительства);
- адрес места пребывания;
- ИНН;
- место работы;
- должность;
- номера контактных телефонов;
- адрес электронной почты;
- образец подписи.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения ООО «ЮРБ» законодательства Российской Федерации в сфере банковской деятельности, валютного регулирования и валютного контроля, противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Я ознакомлен(а), что:

- срок, в течение которого действует настоящее согласие, определяется действующим законодательством Российской Федерации;
- отзыв настоящего согласия производится в письменной форме в соответствии с действующим законодательством Российской Федерации;
- в случае отзыва согласия на обработку персональных данных, ООО «ЮРБ» вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в [пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11](#) Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

Дата начала обработки персональных данных: « _____ » _____ 20____ года

Подпись _____

АКТ приема-передачи USB-токена/ОТР-токена

г. _____ « ____ » _____ 201__ г.

Общество с ограниченной ответственностью «Южный региональный банк», именуемое в дальнейшем «Банк», в лице Председателя правления _____, действующего на основании Устава, с одной стороны, и _____, именуемый(ое) в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», подписали настоящий Акт приема-передачи USB-токена/ОТР-токена (далее – Акт) о том, что:

1. Банк передал, а Клиент получил нижеследующее устройства:

USB-токен, в количестве _____ шт.

ОТР-токен, в количестве _____ шт.

Серийный номер (Идентификатор) ОТР-токена:

№ п/п	Серийный номер (Идентификатор) ОТР-токена
	VASCODigipassGo3 (длина пароля 6 цифр) _____ ActivIdentityMiniOTPToken (длина пароля 8 цифр) _____
	VASCODigipassGo3 (длина пароля 6 цифр) _____ ActivIdentityMiniOTPToken (длина пароля 8 цифр) _____

Серийный номер (Идентификатор) USB-токена:

№ п/п	Серийный номер (Идентификатор) USB-токена

2. Клиент подтверждает, что каждое полученное аппаратное устройство не имеет видимых признаков повреждения и взлома.

3. Клиент обязуется использовать средства электронной подписи в соответствии с Договором на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».

4. Настоящий Акт составлен в двух экземплярах по одному для каждой из Сторон.

БАНК

КЛИЕНТ

_____/_____/_____

_____/_____/_____

М.П.

М.П.

Акт выполненных работ

г. Ростов-на-Дону

« ____ » _____ 201_ г.

Общество с ограниченной ответственностью «Южный региональный банк»,
именуемое в дальнейшем **«Банк»**, в лице **Председателя** правления
_____, действующего на основании
Устава, с одной стороны, и _____

_____,
именуемое в дальнейшем **«Клиент»**, в лице
_____, действующего на основании
_____, с другой стороны, при совместном упоминании
именуемые «Стороны», составили настоящий акт о нижеследующем:

1. Банком были выполнены работы по настройке и подключению Клиента к Системе «iBank2».
2. Клиент принял результаты выполненных Банком работ, претензий к Банку не имеет.
3. Оплата за выполненные работы взимается Банком с Клиента в размере и порядке, предусмотренном в п. 7.2. Договора на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».

4. Адреса и реквизиты Сторон:

БАНК

КЛИЕНТ

Председатель правления

_____/_____/_____/_____/_____

ПОЛОЖЕНИЕ о порядке проведения технической экспертизы при возникновении спорных ситуаций

1. В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки ЭП Клиента под электронным документом.
2. Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ с ЭП, на основании которого Банк выполнил операции по счёту Клиента.
3. Банк обязан в течение не более пяти рабочих дней от даты подачи заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка, выбор членов комиссии осуществляется по согласованию со всеми участниками. При невозможности согласованного выбора, последний проводится случайно (по жребию).
4. Результатом рассмотрения спорной ситуации разрешительной комиссией является определение Стороны, на которую возлагается ответственность согласно выводу об истинности ЭП Клиента под спорным электронным документом.
5. Разрешительная комиссия в течение не более пяти рабочих дней проводит рассмотрение заявления Клиента. Рассмотрение заявления включает следующие этапы:
 - 5.1. Разрешительная комиссия проводит техническую экспертизу с целью установления:
 - электронного документа, заверенного ЭП Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия со счётом Клиента;
 - ключа проверки ЭП Клиента, периода действия и статуса ключа проверки ЭП Клиента, и его принадлежности Клиенту;
 - корректности ЭП Клиента в электронном документе.

Техническая экспертиза проводится с использованием специального программного обеспечения для рассмотрения спорных ситуаций, предоставленного компанией – разработчиком системы «iBank2» - ОАО «БИФИТ».
- 5.2. По требованию одной из Сторон к проведению технической экспертизы может быть привлечена компания – разработчик системы «iBank2» - ОАО «БИФИТ».
- 5.3. На основании данных технической экспертизы разрешительная комиссия составляет акт.
6. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:
 - 6.1. Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по счёту Клиента.
 - 6.2. ЭП Клиента в электронном документе оказалась некорректной.
 - 6.3. Клиент предоставляет уведомление об отмене действия ключа ЭП и соответствующего ему ключа проверки ЭП Клиента, подписанное должностным лицом Банка и имеющим оттиск печати Банка. При этом указанная в уведомлении дата окончания действия пары ключей ЭП Клиента раньше даты, указанной в рассматриваемом электронном документе.
7. В случае, когда Банк предъявляет электронный документ, корректность ЭП Клиента признана разрешительной комиссией, принадлежность Клиенту ключа проверки ЭП Клиента подтверждена, Банк перед Клиентом по выполненным операциям по счёту Клиента ответственности не несёт.

Требования по обеспечению информационной безопасности при работе в системе «iBank2»

Уважаемый Клиент!

В целях обеспечения информационной безопасности при работе в системе «iBank2», необходимо исполнять следующие требования:

1. Реализовать следующие организационные меры защиты информации при назначении функциональных прав и обязанностей сотрудников и использовании средств электронной подписи:

- 1.1. Назначить лиц, допущенных к работе в системе «iBank2» и имеющих право подписи электронных документов.
- 1.2. По возможности запретить доступ к электронному устройству, предназначенному для работы с системой «iBank2» (далее – ЭУ), лиц, не допущенных к работе в системе «iBank2».
- 1.3. Предоставить пользователю, работающему в системе «iBank2» с использованием данного ЭУ, минимальные необходимые права (наличие прав администратора нежелательно).
- 1.4. Не привлекать для администрирования и обслуживания ЭУ, предназначенного для работы в системе «iBank2», технических специалистов на условиях предоставления им удаленного доступа к ЭУ.
- 1.5. Разрешить доступ к НКИ и к другим средствам защиты только сотрудникам, являющимся владельцами ключей ЭП.
- 1.6. Исключить возможность использования НКИ вне ЭУ, предназначенных для работы в системе «iBank2».
- 1.7. Хранить НКИ в месте, недоступном для посторонних лиц. Подключение НКИ к ЭУ допускается только непосредственно на время работы в системе «iBank2». После окончания сеанса работы в системе «iBank2» НКИ должен быть незамедлительно извлечен из ЭУ!
- 1.8. Обеспечить неразглашение паролей, используемых в системе «iBank2». Не передавать пароли к ключам ЭП третьим лицам, не записывать пароли и не сохранять их вместе с НКИ. Не делать простых и легких паролей (111111,12345,abcdefg,qwerty и т.п.). Не следует выбирать в качестве пароля дату рождения, номер телефона и другие данные, которые легко узнать.
- 1.9. Производить замену ключей ЭП до истечения срока их действия. Кроме того, проводить замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к системе «iBank2», а также в случаях подозрений на компрометацию ключей ЭП.

2. Реализовать следующие технологические меры защиты информации:

2.1. Использовать на ЭУ только лицензионное ПО. Своевременно устанавливать обновления операционной системы ЭУ, рекомендуемые компанией-производителем, в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления (установка патчей) Web - браузера и ПО Java на ЭУ, так как данные действия значительно повысят его уровень безопасности. Для обновления системного и прикладного ПО необходимо использовать только источники, гарантирующие отсутствие вредоносных программ.

2.2. На ЭУ, используемых для работы в системе «iBank2», рекомендуется выполнить следующие настройки:

- Запретить в свойствах Web - браузера:
 - автоматическую загрузку файлов из сети Интернет;
 - автоматический запуск файлов из сети Интернет;
 - автоматическую загрузку не подписанных элементов ActiveX.
- Отключить загрузку с гибкого диска, привода CD-ROM, загрузку с внешних USB-носителей, загрузку по сети.
- Отключить учетную запись для гостевого входа (Guest/Гость).
- Исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке.
- Отключить режимы отображения окна всех зарегистрированных на ЭУ пользователей и быстрого переключения пользователей.
- Запретить в настройках операционной системы удаленный доступ к этому ЭУ.

3. Реализовать следующие меры для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования ЭУ (далее – вредоносный

код):

3.1. Установить и регулярно обновлять на ЭУ следующие лицензионные технические средства защиты информации, предназначенные для предотвращения воздействия вредоносного кода:

- антивирусное программное обеспечение с ежедневно обновляемыми базами данных сигнатур вредоносных кодов;
- персональные межсетевые экраны (firewall);
- средства защиты от несанкционированного доступа и пр.

3.2. Использовать дополнительное программное обеспечение, позволяющее повысить уровень защиты ЭУ – программы поиска шпионских компонент, программы защиты от «спам» - рассылки.

4. Реализовать следующие меры для защиты информации при использовании сети Интернет:

4.1. На ЭУ, используемых для работы в системе «iBank2», исключить посещение Интернет-сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), загрузку и установку нелицензионного ПО, и т. п.

4.2. Не работать в системе «iBank2» из мест, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.).

4.3. При работе в системе «iBank2» убедиться, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (<https://ibank2.ru>), не переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка, www.urb.ru) или поступивших по электронной почте писем.

4.4. Ограничить список IP-адресов, с которых будет разрешена работа в системе «iBank2». Наиболее предпочтительно использовать при работе в системе «iBank2» статические IP-адреса, что позволяет задействовать встроенный в систему механизм IP-фильтрации в полной мере.

4.5. В случае появления предупреждений Web - браузера о перенаправлении Вас на другой сайт при подключении к системе «iBank2» отложить совершение операций и обратиться в службу технической поддержки Банка.

5. Предпринимать следующие дополнительные меры защиты информации при осуществлении работы в системе «iBank2»:

5.1. При входе в систему «iBank2» обращать внимание на информацию о последних сеансах работы в системе «iBank2». Данная информация включает в себя дату и время сеанса, номер ключа и IP-адрес, с которого осуществлялся сеанс. Если информация не соответствует Вашим действиям в системе «iBank2», нужно незамедлительно поставить об этом в известность службу технической поддержки Банка с целью блокировки ключей ЭП.

5.2. Если при входе в систему «iBank2» окно для ввода пароля отличается от стандартных окон системы «iBank2» (логотип другого банка, другие надписи, шрифт и т.д.) или отображается не так как всегда (нарушен порядок работы в системе «iBank2»), не вводить имена и пароли.

5.3. В случае сбоев в работе ЭУ или его поломки во время/после работы в системе «iBank2» (проблемы с загрузкой операционной системы, выход из строя жесткого диска, «странное» поведение ЭУ, медленная работа), следует **НЕМЕДЛЕННО** извлечь НКИ и выключить ЭУ, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.

5.4. Обращать внимание на любые изменения в привычных процессах установления соединения с системой «iBank2» или в функционировании системы «iBank2». При возникновении любых сомнений в правильности функционирования системы «iBank2» незамедлительно обращаться в Банк.

5.5. Не отвечать на письма с просьбой выслать ключ ЭП и пароль. Банк никогда не запрашивает у Клиентов такую информацию. Такое письмо может быть направлено только злоумышленниками с целью завладеть Вашим ключом ЭП.

5.6. Регулярно контролировать состояние счетов, зарегистрированных в системе «iBank2», и незамедлительно сообщать сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

ВНИМАНИЕ!

Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств с Ваших счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.

При любых подозрениях на мошеннические действия (компрометацию ключей ЭП, логинов, паролей и т.д.), а также при нестабильной работе системы «iBank2» (зависание системы «iBank2», самопроизвольное выключение системы «iBank2», ЭУ и т.д.), следует незамедлительно прекратить работу в системе «iBank2», извлечь из ЭУ НКИ, и обратиться в Банк.

Настоящие Требования по обеспечению информационной безопасности при работе в системе «iBank2» являются обязательными для исполнения и соблюдения Клиентом!

Порядок уведомления Клиента о совершении операций в системе «iBank2»

1. Способом уведомления Клиента о:
 - поступлении распоряжений и иных ЭД Клиента в Банк Стороны признают присвоенный ЭД в системе «iBank2» **статус «Доставлено»**;
 - поступлении распоряжений и иных ЭД Клиента на исполнение Стороны признают присвоенный ЭД в системе «iBank2» **статус «На обработке»**;
 - об исполнении Банком распоряжений и иных ЭД Клиента, Стороны признают присвоенный ЭД в системе «iBank2» **статус «Исполнен»**;
 - об отклонении Банком распоряжений и иных ЭД Клиента, Стороны признают присвоенный ЭД в системе «iBank2» **статус «Отвергнут»**.
2. В целях исполнения требований федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» в системе «iBank2» используется сервис «Мониторинг», посредством которого осуществляется дополнительное информирование Клиента путем рассылки SMS-сообщений и/или E-mail-сообщений о следующих операциях:
 - вход Клиента в систему «iBank2»;
 - поступление в Банк расчетного документа Клиента;
 - отклонение Банком расчетного документа Клиента.
3. Доступ Клиента к сервису «Мониторинг» осуществляется на основании настоящего Договора одновременно с регистрацией счетов Клиента в системе «iBank2».
4. Уведомление Клиента об операциях в системе «iBank2» осуществляется одним или двумя из следующих способов:
 - путем отправки sms-сообщений на номера мобильных телефонов, указанные Клиентом в Заявлении (Оферте) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2»;
 - путем отправки сообщений по E-mail на адреса электронной почты, указанные в Заявлении (Оферте) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».
5. Фактом уведомления Банком Клиента об операциях в системе «iBank2», перечисленных в п. 2 настоящего Порядка, Стороны признают наличие записи о соответствующей операции в Детальном отчете Статистики по уведомлениям модуля «Мониторинг» системы «iBank2».
6. В случае изменения номера мобильного телефона и/или утери SIM-карты, Клиент обязан уведомить об этом Банк в письменном виде.
7. Банк не несет ответственности за задержки и сбои, возникающие в сетях операторов сотовой связи и сервисах провайдеров, которые могут повлечь за собой задержку или недоставку SMS/E-Mail-сообщений Клиенту.
8. Телекоммуникационные каналы, используемые для передачи SMS/E-Mail-сообщений, являются открытыми и не гарантируют полную защиту информации. Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну.
9. Все рассылаемые сервисом «Мониторинг» сообщения носят информационный характер.

Требования к аппаратно-программному обеспечению Клиента для работы в системе «iBank2»

Банк устанавливает следующие требования к программно-техническим средствам, необходимым Клиенту для подключения и работе в системе «iBank2»:

1. Наличие электронного устройства (персональный компьютер, ноутбук, планшетный компьютер и т.п.) с любой операционной системой, Web-браузером и виртуальной Java-машиной — Sun Java, Java for Mac OS X или любой другой, не ниже Java 6 (далее – ЭУ).

Для установки на ЭУ Клиента виртуальной Java-машины необходимо получить по адресу: <http://www.java.com/ru> дистрибутив последней версии минимальной реализации виртуальной машины, необходимой для исполнения Java-приложений, без компилятора и других средств разработки (JRE) для используемой операционной системы.

2. Наличие доступа в сеть Интернет. Рекомендуемая скорость соединения — 33,6 Кбит/сек и выше. В случае доступа в сеть Интернет по телефонной коммутируемой линии необходимо наличие модема.

3. Обязательное использование при подключении по выделенному каналу межсетевого экрана – Firewall, осуществляющего фильтрацию пакетов в соответствии с правилами, заданными администратором.

Исходя из этого, для работы Java-апплетов в правилах фильтрации на Firewall необходимо открыть следующие TCP-порты:

- 443 TCP-порт для соединения Web-браузера на ЭУ Клиента с Web-сервером Банка по протоколу SSL;
- 443 TCP-порт для работы Java-апплета «Internet-Банкинг для корпоративных клиентов с сервером системы «iBank2».

4. Наличие принтера, на котором после завершения процедуры генерации ключей ЭП Клиента необходимо будет распечатать Сертификат ключа проверки ЭП Клиента.

5. Наличие в ЭУ Клиента USB-порта, позволяющего Клиенту использовать USB-токен - персональный аппаратный криптопровайдер.

6. Наличие на ЭУ Клиента лицензионного антивирусного программного обеспечения с актуальными, ежедневно обновляемыми базами данных, содержащими описание вредоносных кодов и способы их обезвреживания.

Порядок действий Сторон в случае выявления хищения денежных средств в системе «iBank2»

1. Клиенту в случае выявления хищения денежных средств в системе «iBank2» необходимо:

1.1. Немедленно прекратить любые действия с ЭУ, подключенным к системе «iBank2», обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.) или перевести в режим гибернации («спящий» режим).

При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.

1.2. При наличии технической возможности отозвать распоряжение на перевод денежных средств с использованием иного ЭУ, после чего принять меры к блокировке системы «iBank2».

1.3. При отсутствии технической возможности отозвать распоряжение на перевод денежных средств по системе «iBank2» немедленно обратиться в Банк по контактным телефонам, указанным в Заявлении (Оферте) о присоединении к Договору на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2», с заявлением о блокировке системы «iBank2», приостановке исполнения распоряжения на перевод денежных средств и возврате денежных средств.

1.4. Произвести фотосъемку ЭУ (с подключенными кабелями и иными периферийными устройствами), рабочего места и его расположения в помещении. Обеспечить сохранность (целостность) ЭУ как возможного средства совершения преступления, поместив его в место с ограниченным доступом, обеспечив при этом защиту от вскрытия (стикеры, наклейки, пластилин, мастичная печать, пломбы и т.п.) и по возможности зафиксировать средства контроля целостности фотографированием со всех ракурсов. Если позволяют размеры ЭУ, следует поместить его в непрозрачный пакет (мешок) и заклеить горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

1.5. Дополнительно к действиям, перечисленным в пп. 1.2., 1.3. настоящего Порядка, обратиться в Банк с письменным заявлением об отзыве распоряжения на перевод денежных средств, возврате денежных средств и блокировании доступа к системе «iBank2» (Приложение № 11.1. к настоящему Договору), а также о компрометации ключей ЭП и необходимости смены ключей ЭП. Копия заявления должна быть направлена в Банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в Банк течение одного дня.

1.6. Проинформировать все кредитные организации, с которыми Клиент имеет договорные отношения, предусматривающие использование систем ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

1.7. При наличии необходимой информации обратиться в банк-получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении зачисления денежных средств на счет получателя и возврате денежных средств (Приложение № 11.2. к настоящему Договору).

1.8. 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 (при наличии таковых) за максимальный период времени, как до, так и после даты совершения хищения денежных средств.

1.9. Провести сбор записей с межсетевых экранов и других средств защиты информации, серверов баз данных и иных компонент клиентского приложения системы «iBank2», систем авторизации пользователей (AD, NDS и т.д.), коммуникационного оборудования (включая АТС), ЭУ, устройств, которые могут использоваться для удаленного управления указанными ЭУ.

1.10. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи (Приложение № 11.3. к настоящему Договору) для получения в электронной форме журналов соединений с сетью Интернет с ЭУ клиента или из его локальной вычислительной сети (далее - ЛВС) как минимум за три месяца, предшествовавшие факту хищения денежных средств.

1.11. Не предпринимать никаких действий для самостоятельного или с привлечением сторонних ИТ-специалистов поиска и удаления компьютерных вирусов, восстановления работоспособности ЭУ, не отправлять ЭУ в сервисные службы для восстановления работоспособности.

1.12. Зафиксировать в протокольной форме значимые действия и события, в том числе имена лиц, имеющих доступ к ЭУ, действия с ЭУ, подключенным к системе «iBank2», предшествовавшие факту хищения денежных средств, подготовить объяснения работников Клиента об использовании ЭУ в целях, отличных от осуществления операций в системе «iBank2», посещаемых интернет-сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в Банк, о сторонних лицах, побывавших в

месте расположения ЭУ и т.д.

1.13. Все действия, указанные в пп. 1.1., 1.4., 1.8., 1.9., 1.12. настоящего Порядка, производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъемки.

При невозможности осуществления коллегиальных действий отдельно зафиксировать данный факт.

1.14. Оперативно обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (Приложение № 11.4. к настоящему Договору).

1.15. Оперативно обратиться в суд с исковым заявлением в отношении получателя денежных средств (указав все известные реквизиты получателя) о взыскании неосновательно полученного обогащения и процентов за пользование денежными средствами (глава 60 ГК РФ), а также с ходатайством о принятии судом мер по обеспечению иска в виде ареста денежных средств на счете получателя в сумме неосновательно полученного обогащения. К исковому заявлению необходимо приложить копию заявления о возбуждении уголовного дела либо копию талона, содержащего порядковый номер из книги учета сообщений о преступлениях (далее - КУСП) содержащую отметку правоохранительного органа о его приеме.

1.16. Копии вышеуказанных документов направить в Банк с приложением Справки по факту инцидента информационной безопасности в системе «iBank2» (Приложение № 11.5. к настоящему Договору), а также подтверждающих документов (Приложение № 11.6. к настоящему Договору).

2. Сотрудники Банка в случае выявления хищения денежных средств в системе «iBank2»:

2.1. При получении телефонного обращения Клиента-плательщика о приостановке исполнения распоряжения о переводе денежных средств немедленно предпринимают разумно возможные и достаточные действия для идентификации Клиента-плательщика, в том числе, посредством использования контактной информации, указанной в договоре банковского счета. При наличии возможности используют дополнительные каналы для подтверждения обращения (SMS-уведомление, сообщение по электронной почте).

2.2. При подтверждении обращения Клиента незамедлительно принимают меры к приостановке дальнейшей обработки платежа. При невозможности аутентификации Клиента-плательщика, фиксируют данный факт, и продолжают обработку платежа, если нет иных оснований для приостановки дальнейшей обработки платежа.

2.3. В случае завершения обработки платежа незамедлительно в любой доступной форме направляют в службу безопасности банка-получателя информацию о факте хищения денежных средств с просьбой о приостановке обработки платежа.

2.4. Оперативно направляют с использованием сервисов расчетной системы Банка России в банк-получателя сообщение с просьбой о приостановлении платежа и возврате денежных средств.

2.5. С целью обеспечения сохранности доказательств исключают доставку в Банк и/или техническое обслуживание ЭУ Клиента, консультации, проверки ЭУ Клиента, а равно совершение сотрудниками Банка иных действий, которые могут привести к нарушению сохранности доказательств.

2.6. Оперативно направляют письмо в банк-получателя или оператору платежной системы по факту хищения денежных средств с просьбой о прекращении обработки платежа, блокировке системы ДБО и платежных карт клиента - получателя, применении к получателю платежа мер контроля в рамках системы ПОД/ФТ, предусмотренных Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», и возврате денежных средств.

Истребуют у Клиента-плательщика подтверждение о подаче Клиентом-плательщиком заявления в правоохранительные органы для получения его копии в течение не более 2 рабочих дней со дня получения обращения Клиента-плательщика в Банк о факте хищения денежных средств.

2.7. Подготавливают документы, указанные в Приложении № 11.7. к настоящему Договору.

2.8. Осуществляют следующие действия с привлечением сотрудников отдела информационной безопасности:

2.8.1. Проводят мероприятия, определенные настоящим Договором, в отношении проверки подлинности ЭП под оспоренным расчетным документом. При необходимости - проводят мероприятия по факту компрометации ключей ЭП.

2.8.2. Получают от сотрудников Банка, ответственных за обслуживание системы «iBank2», администраторов сети, систем криптографической защиты и т.д. экспертные заключения в рамках их компетенции по корректности ЭП в составе расчетного документа, ее целостности и авторства.

2.8.3. Проводят анализ собранной информации с целью выявления источника осуществления хищения денежных средств и возможной причастности сотрудников Банка. Документально оформляют результаты проверки.

2.8.4. При необходимости - проводят технические мероприятия, направленные на предотвращение сокрытия следов, уничтожения информации и т.д., для чего задействуют используемые в Банке средства и методы защиты информации.

2.8.5. Обеспечивают хранение собранной информации в неизменном виде для передачи

правоохранительным органам по запросу.

2.9. При необходимости проводят, документально зафиксировав полученные результаты, следующие проверочные мероприятия в целях формирования необходимой доказательной базы по факту хищения денежных средств:

2.9.1. Находят оспоренный Клиентом-плательщиком расчетный документ в базе данных системы «iBank2» и в базе данных автоматизированной банковской системы (далее - АБС) Банка.

2.9.2. Если расчетный документ не найден в базе данных «iBank2», но имеется в базе данных АБС Банка:

2.9.2.1. По журналам систем «iBank2» и АБС устанавливают, присутствовал ли расчетный документ в системе «iBank2» ранее.

2.9.2.2. В свойствах расчетного документа устанавливают его авторство, дату, время и способ его создания.

2.9.2.3. Получают объяснения от сотрудников Банка, уполномоченных на оформление и проверку расчетных документов, администраторов «iBank2» и АБС Банка, администраторов информационной безопасности «iBank2» и АБС Банка.

2.9.2.4. Проводят сбор записей с межсетевых экранов, систем обнаружения вторжений и антивирусной защиты, серверов баз данных, систем авторизации пользователей (AD, NDS и т.д.), рабочих станций сотрудников Банка, штатно допущенных к управлению системой «iBank2», и средств удаленного управления указанными рабочими станциями.

2.9.2.5. Получают записи систем видеонаблюдения, управления доступом в помещения Банка и т.д.

2.9.2.6. Оценивают возможность продолжения эксплуатации системы «iBank2».

2.9.3. Если расчетный документ найден в базе данных системы «iBank2», проверяют подлинность оспариваемого расчетного документа.

2.9.3.1. Если подлинность расчетного документа не установлена:

2.9.3.1.1. Получают объяснения от сотрудников Банка, уполномоченных на оформление и проверку расчетных документов, поступивших по системе «iBank2», администраторов системы «iBank2» и АБС Банка, администраторов информационной безопасности системы «iBank2» и АБС Банка.

2.9.3.1.2. По журналам системы «iBank2» устанавливают, была ли подлинность расчетного документа утрачена в процессе эксплуатации системы «iBank2», а также оценивают возможность продолжения эксплуатации системы «iBank2».

2.9.3.2. Если подлинность расчетного документа установлена:

2.9.3.2.1. Реализовывают неотложные действия при компрометации ключа ЭП Клиента-плательщика непосредственно после обращения Клиента.

2.9.3.2.2. Получают от уполномоченного сотрудника Банка журналы работы системы «iBank2» и анализируют их на предмет наличия записей, содержащих признаки несанкционированного доступа посторонних лиц.

2.9.3.2.3. Проводят мероприятия, направленные на обеспечение целостности носителя.

2.9.4. Проводят анализ информации с целью выявления возможной причастности к хищению денежных средств сотрудников Банка. При необходимости проводят технические мероприятия, направленные на предотвращение сокрытия следов хищения.

2.10. Получают от Клиента-плательщика Справку по факту инцидента информационной безопасности в системе «iBank2» (Приложение № 11.5. к настоящему Договору).

2.11. На основании собранной информации оформляют и передают в правоохранительный орган, осуществляющий расследование по факту хищения денежных средств, объяснение по факту хищения денежных средств. В случае отказа Клиента-плательщика от обращения в правоохранительные органы оформляют обращение по факту хищения денежных средств в региональное подразделение МВД от имени Банка.

2.12. Обращаются в Бюро специальных технических мероприятий Главного Управления МВД России с заявлением об оказании содействия в расследовании факта хищения денежных средств с подробным описанием обстоятельств его совершения, по запросу БСТМ МВД России направляют документы, указанные в Приложении № 11.7. к настоящему Договору.

2.13. В случае хищения денежных средств Клиента-плательщика, по счетам которого зафиксированы поступления средств бюджета любого уровня, также направляют информационное письмо на имя руководителя ФСБ России о факте хищения денежных средств с подробным описанием обстоятельств его совершения.

2.14. Направляют в банк-получателя полученную от Клиента-плательщика копию заявления в правоохранительный орган по факту хищения денежных средств и номер КУСП (в случае обращения в правоохранительные органы).

2.15. При наличии в Банке электронного расчетного документа Клиента с подлинной электронной подписью и при оспаривании подлинности электронной подписи в составе электронного расчетного документа, подтверждающего поручение Клиента-плательщика Банку выполнить оспоренный перевод, направляют Клиенту-плательщику письмо о готовности участия в работе экспертной комиссии с целью проверки подлинности электронной подписи.

ЗАЯВЛЕНИЕ

Настоящим сообщаем, что «____» _____ 201__ года с банковского счета № _____, открытого в _____, по системе дистанционного банковского обслуживания «iBank 2» были похищены денежные средства, которые, по имеющейся информации были переведены по следующим платежным реквизитам:

Дата платежа	«____» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Прошу Вас заблокировать ключи электронной подписи со следующими идентификационными номерами _____ в системе дистанционного банковского обслуживания «iBank 2» и оказать содействие в возврате денежных средств.

должность

подпись

(_____)

расшифровка подписи

«____» _____ 20__ года

Исп. _____

Ф.И.О.

тел. _____

должность руководителя

наименование банка-получателя

Ф.И.О. руководителя

ЗАЯВЛЕНИЕ

Настоящим сообщаем, что «___» _____ 201__ года с нашего банковского счета № _____, открытого в _____ (БИК _____) были похищены денежные средства, которые, по информации, полученной из ООО «ЮРБ», были переведены со следующим реквизитам платежа:

Дата платежа	«___» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Прошу Вас оказать содействие в приостановлении прохождения платежа и возврате денежных средств.

должность

подпись

(_____)

расшифровка подписи

«___» _____ 20__ года

Исп. _____

Ф.И.О.

тел. _____

должность руководителя

наименование организации-провайдера

Ф.И.О. руководителя

«___» _____ 20__ года между _____ и вами был заключен договор N _____ об оказании _____ услуг.

Настоящим сообщая, что «___» _____ 20__ года в __:__ по московскому времени с расчетного счета _____ (далее – Счет), по системе дистанционного банковского обслуживания (далее – система ДБО) был осуществлен несанкционированный перевод денежных средств.

Компьютер, с которого осуществляется подключение к системе дистанционного банковского обслуживания (далее – ДБО), располагается по адресу: _____ и использует IP-адрес _____ (далее – Компьютер).

Вероятной причиной несанкционированного перевода денежных средств со Счета могло послужить заражение Компьютера вредоносным программным обеспечением, кража логина, пароля и ключей электронной подписи системы ДБО.

Для выявления обстоятельств несанкционированного перевода денежных средств со Счета прошу предоставить информацию из журналов (логов) о входящем и исходящем трафике за период с «___» _____ 20__ года по «___» _____ 20__ года с указанием времени соединения, IP и MAC адресов.

должность

подпись

(_____)

расшифровка подписи

«___» _____ 20__ года

Исп. _____
Ф.И.О.

тел. _____

Начальнику ОВД по _____
наименование ОВД
от _____
должность, ФИО заявителя

наименование организации

ЗАЯВЛЕНИЕ

Прошу провести проверку настоящего заявления по факту незаконного завладения принадлежащими _____
наименование организации/ФИО потерпевшего
денежными средствами (кражи) с использованием системы дистанционного банковского обслуживания (далее - ДБО) ООО «ЮРБ».
«___» _____ 201__ г. неизвестными лицами по системе ДБО был осуществлен несанкционированный перевод денежных средств со следующими реквизитами:

Дата платежа	«___» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Оснований для данного денежного перевода нет: с получателем платежа отсутствуют договорные и иные деловые отношения, равно как и какие-либо обязательства перед ним; перевод расцениваю как хищение денежных средств.

Признаком хищения является то, что этот перевод не был осуществлен уполномоченными лицами.

Факт осуществления этого перевода был установлен «___» _____ 201__ г.

ФИО лица, установившего факт несанкционированного перевода,
должность, наименование организации
при _____
обстоятельства обнаружения факта несанкционированного перевода

Компьютер, с которого осуществляется подключение к системе ДБО, располагается по адресу: _____, доступ к электронному устройству ограничен, прямая кража учетной записи, пароля и ключей электронной подписи маловероятна.

Вероятной причиной этого несанкционированного перевода денежных средств считаю ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, поскольку данному событию сопутствовали следующие обстоятельства:

1. _____;
обстоятельства, снижающие вероятность прямого хищения реквизитов доступа в систему ДБО
2. _____;
наблюдавшиеся сбои, нехарактерное поведение системы ДБО и рабочего места системы ДБО
3. _____.
иное

На основании изложенного, прошу Вас провести необходимые оперативно-розыскные мероприятия для выявления виновных лиц и привлечь их к уголовной ответственности в соответствии с действующим законодательством.

_____ (_____)
должность подпись расшифровка подписи
«___» _____ 20__ года

Исп. _____, тел. _____

Справка по факту инцидента информационной безопасности в системе «iBank2»

Настоящим сообщаяю, что «___» _____ 20__ года неустановленным лицом через систему «iBank 2» была совершена несанкционированная операция по переводу денежных средств со следующими реквизитами:

Дата платежа	«___» _____ 201__ г.
Номер распоряжения	
Наименование банка плательщика	
Наименование плательщика	
ИНН плательщика	
Номер счета плательщика	
Наименование банка получателя	
Наименование получателя	
ИНН получателя	
Номер счета получателя	
Сумма платежа	
Назначение платежа	

Дополнительно сообщаяю:

1. Количество ЭУ, используемых для доступа в систему «iBank 2»: _____.
2. Для доступа в систему «iBank 2» хотя бы раз использовались:
 - корпоративные ЭУ
 - личные ЭУ
 - ЭУ, находящиеся в общественном пользовании.
3. Периодичность смены пароля для входа в систему «iBank 2»: _____.
4. Применяемые элементы безопасности ЭУ включают:
 - используется только программное обеспечение для работы в системе «iBank 2»
 - используется только лицензионное программное обеспечение
 - операционная система и приложения обновляются в автоматическом режиме
 - используется антивирусное программное обеспечение: _____
 - антивирусное программное обеспечение обновляется ежедневно
 - из числа съемных носителей информации на ЭУ используются только носители ключевой информации
 - передача файлов и обмен сообщениями по электронной почте на ЭУ ограничены
 - используются средства сетевой защиты: _____
 - на ЭУ запрещены входящие соединения из сети Интернет
 - запрещено удаленное управление ЭУ
 - с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов сети Интернет для проведения обновлений программного обеспечения, число разрешенных сайтов составляет _____
 - обеспечивается возможность доступа к ЭУ только уполномоченных лиц

- обеспечивается возможность доступа к носителям ключевой информации только уполномоченных лиц
- часы работы Клиента
- список лиц, имеющих доступ к НКИ
- список лиц, имеющих доступ к ЭУ

Иная информация, имеющая отношение к инциденту:

_____ (_____)
 должность подпись расшифровка подписи

_____ **намерено** обратиться в правоохранительные органы по факту хищения денежных средств
 (название Клиента)

Заявление в правоохранительные органы принято в ОВД

район, округ, город, субъект федерации и иные идентифицирующие ОВД данные и зарегистрировано за N _____ в КУСП

_____ **не намерено** обратиться в правоохранительные органы по факту хищения денежных средств
 (название Клиента)

О необходимости предоставления доступа сотрудников правоохранительных органов к электронному устройству предупрежден.

_____ (_____)
 должность подпись расшифровка подписи

«__» _____ 20__ года

Исп. _____, тел. _____

Перечень документов, которые могут быть истребованы у клиента-плательщика в случае выявления хищения денежных средств

1. Копия лицензии на операционную систему электронного устройства (далее – ЭУ).
2. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы).
3. Копия договора на оказание телематических услуг информационно-телекоммуникационной сети Интернет.
4. Описание организации доступа в сеть Интернет на рабочем месте.
5. Копия заявления в правоохранительные органы.
6. Копия лицензии на антивирусное ПО.
7. Копия документа, подтверждающего легальность антивирусного ПО.
8. Описание средств антивирусной защиты рабочего места (наличие установленного на жестком диске ЭУ Клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на ЭУ Клиента вредоносных программ и пр.).
9. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у Клиента, сведения об использовании рабочего места в иных целях, кроме осуществления операций в системе «iBank2», в частности - интернет-серфинга, сведения о порядке хранения и использования носителей ключевой информации).

**Перечень документов в отношении потерпевшего Клиента, на счет которого
неправомерно зачислены денежные средства**

1. Договор банковского счета, договор на обслуживание Клиента в системе дистанционного банковского обслуживания «iBank2».
2. Сведения о точном месте открытия и месте нахождения счета Клиента.
3. Заверенная копия карточки с образцами подписей и оттиска печати Клиента.
4. Расширенная выписка по Счету Клиента с отражением сведений о движении денежных средств в период осуществления несанкционированного перевода.
5. Заверенные копии платежных документов, на основании которых были несанкционированно переведены денежные средства.
6. Носитель информации, содержащий записи видеокамер, имеющие отношение к хищению (до процессуального изъятия оригинала технического носителя информации следует обеспечить сохранность записей).
7. Документы, отражающие статистику соединений с системой «iBank2», с указанием учетных записей, внешних IP-адресов Клиента и точного времени соединений в период осуществления несанкционированного перевода.
8. Сведения о представителях Клиента, имеющих право подписи, в том числе электронной подписи расчетных документов.
9. Сведения о подключенных уведомительных услугах Банка (СМС-уведомление, голосовая авторизация, уведомление на электронную почту, привязка к выделенному IP-адресу и другие имеющиеся услуги) с приложением копий документов, акцептованных Банком при предоставлении указанных услуг.
10. Материалы, подготовленные Банком по итогам проведения внутренних проверок.