*Приложение №3 к Единому договору*

*банковского обслуживания*

**УСЛОВИЯ**

**предоставления услуг с использованием системы дистанционного банковского обслуживания (ДБО) юридическим лицам, индивидуальным предпринимателям или физическим лицам, занимающимся в установленном действующим законодательством Российской Федерации порядке частной практикой.**

1. **ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

**Банк** – Публичное акционерное общество «Балтийский Инвестиционный Банк» (сокращенное наименование – ПАО «БАЛТИНВЕСТБАНК»), его филиалы и структурные подразделения.

Клиент – Юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся в установленном действующим законодательством Российской Федерации порядке частной практикой, заключивший Договор о предоставлении услуг с использованием системы дистанционного банковского обслуживания (ДБО).

Договор – комплект следующих документов: «Заявление на заключение договора о предоставлении услуг с использованием системы ДБО» (Приложение 5) и «Условия предоставления услуг с использованием системы ДБО юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном действующим законодательством Российской Федерации порядке частной практикой»

Акт признания ключа проверки электронной подписи - документ на бумажном носителе, выданный Банком и подтверждающий принадлежность ключа проверки электронной подписи Клиенту-владельцу сертификата ключа проверки электронной подписи, содержащий полный текст открытого ключа.

Заявление на заключение договора – Заявление на заключение договора о предоставлении услуг с использованием системы ДБО, являющееся акцептом предложенной Банком оферты на заключение договора.

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

**Сертификат ключа проверки электронной подписи -** электронный документ или документ на бумажном носителе, выданные Банком и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

**Ключ электронной подписи –** уникальная последовательность символов, предназначенная для создания электронной подписи.

**Ключ проверки электронной подписи –** уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности ЭП.

**Система дистанционного банковского обслуживания** (далее по тексту Система ДБО)— комплекс программно-технических средств, осуществляющий функции:

* подготовки и передачи Клиентом в Банк документов в электронном виде (далее по тексту - **электронные документы, ЭД**), содержащих ЭП, позволяющую удостоверять подлинность документа, включая все его обязательные реквизиты;
* передачи электронных документов для дальнейшей обработки в автоматизированную банковскую систему;
* контроля, обработки Банком электронных документов;
* формирования Банком и предоставления Клиенту по каналам связи выписки о движении средств, справки о состоянии счета, данных об изменении реквизитов банков и прочих сообщений.
* официального информирования Банком Клиента путем передачи текстовых сообщений.

**Подсистема «Банк-Клиент»**— часть программного обеспечения Системы ДБО (ДБО BS-Client v.3), устанавливаемая на вычислительные средства Клиента и предназначенная для обмена электронными документами и иной информацией между Банком и Клиентом.

**Подсистема «Интернет-Клиент»** (Интернет-Клиент)— часть программного обеспечения Системы ДБО, позволяющая осуществлять функции обмена электронными документами и иной информацией с использованием стандартных средств работы с Интернет-страницами.

**Электронный документ** (далее по тексту ЭД)– электронный образ документа (платежного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа.

**Электронное средство платежа (**далее по тексту **ЭСП)** - средство и (или) способ, позволяющие клиенту банка составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий.

**Электронный расчетный документ**  ЭРД - электронный документ (платежное поручение Клиента в электронном виде), являющийся основанием для совершения Банком операций по банковскому счету Клиента и подписанное ЭП. Подлинником электронного расчетного документа является любой файл в оговоренном Сторонами формате, который содержит текст документа и ЭП уполномоченных лиц Сторон, подписавших документ, при условии положительного результата проверки подлинности ЭП, произведенной Системой ДБО, с использованием ключей проверки ЭП, зарегистрированных в установленном настоящим Договором порядке. Документом, предназначенным для целей документарного учета, является бумажная распечатка файла, содержащего документ, полученная средствами Системы ДБО на стороне Банка, с физической подписью уполномоченного сотрудника и удостоверенная штампом Банка.

**Стороны** – стороны по договору присоединения: Банк и Клиент

**Сторона-отправитель** – сторона по Договору, Банк либо Клиент, направившая электронный документ по системе ДБО.

**Сторона-получатель -** сторона по Договору, Банк либо Клиент, получившая электронный документ по системе ДБО.

**Счет** – расчетный счет, счет по депозиту, открытый Банком Клиенту, к которому Клиенту предоставлен доступ с использованием Системы ДБО.

**SMS-авторизация***–*подтверждение входа в Подсистему «Интернет-Клиент» посредством ввода одноразового пароля, направляемого Банком на мобильный телефон Уполномоченного лица Клиента.

**Одноразовый пароль -** уникальный цифровой код, направляемый в виде SMS-сообщения на мобильное устройство Уполномоченного лица Клиента. Применяется один раз в определенный момент времени при входе в «Интернет-Клиент». Время, в течение которого осуществляется доставка кода с помощью SMS-сообщения, зависит от оператора мобильной связи и местоположения абонента. Одноразовый пароль действителен на протяжении ограниченного периода времени[[1]](#footnote-1) и однозначно соответствует сеансу использования системы «Интернет-Клиент» или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы «Интернет-Клиент».

**Условия -** Условия предоставления услуг с использованием системы дистанционного банковского обслуживания (ДБО) юридическим лицам, индивидуальным предпринимателям и физическим лицам, занимающимся в установленном действующим законодательством Российской Федерации порядке частной практикой.

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Обслуживание Банком Клиентов осуществляется на основании заключенных Договоров в соответствии с Тарифами Банка.
   2. Заключение Договора между Банком и Клиентом осуществляется путем присоединения Клиента к настоящим Условиям (акцепта Условий) в соответствии со статьей 428 Гражданского кодекса Российской Федерации и производится путем передачи Клиентом в Банк Заявления на заключение Договора.
   3. Заключение Договора осуществляется после предоставления Клиентом в Банк всех документов и сведений, установленных действующим законодательством Российской Федерации
   4. Фактом заключения Договора является подача Клиентом в Банк Заявления на заключение Договора.
   5. Настоящие Условия регламентируют порядок и условия оказания услуг Клиентам с использованием Системы ДБО.
   6. Банк предоставляет Клиенту с использованием Системы ДБО следующие услуги, в том числе на платной основе, предусмотренные Тарифами Банка:

* прием от Клиента ЭРД, на выполнение операций по Счету/Счетам Клиента;
* прием от Клиента и предоставление Клиенту информации в форме ЭД, в том числе предоставление Клиенту информации об операциях, совершенных по Счету/Счетам Клиента;
* прием от Клиента и предоставление Клиенту ЭД в соответствии с условиями отдельных заключенных Сторонами договоров, которые предусматривают электронный документооборот с использованием Системы ДБО;
* обмен между Клиентом и Банком документами и информацией в электронном виде, связанными с проведением валютных операций, требование о представлении (направлении) которых предусмотрено действующими нормативно-правовыми актами валютного законодательства);
* прием от Клиента и предоставление Клиенту информации свободного формата в виде ЭД;
* заключение Договоров/Соглашений средствами Системы в рамках реализованных форм электронных документов;
* прием Банком в обработку подписанных ЭП электронных документов от Клиента;
  1. Стороны договорились использовать следующие электронные документы:
* платежное поручение на перевод средств в рублях;
* поручение на перевод валюты;
* поручение на обязательную продажу иностранной валюты;
* поручение на продажу иностранной валюты;
* поручение на покупку иностранной валюты;
* поручение на конверсию иностранной валюты;
* заявление об акцепте, отказе от акцепта;
* выписки со счетов Клиента в валюте Российской Федерации и иностранной валюте;
* справка о валютных операциях;
* запрос на выписку;
* уведомление Банка о совершенных операциях;

- уведомление о поступлении валюты в произвольной форме;

* запрос на отзыв документа;
* паспорт сделки по контракту;
* паспорт сделки по кредитному договору;
* справка о подтверждающих документах;
* заявление о переоформлении паспорта сделки;
* заявление о закрытии/переводе паспорта сделки;
* заявление на депозит (только в Подсистеме «Интернет-Клиент»);
* произвольные документы.
  1. Применение электронных платежных документов не отменяет установленных законодательством и другими договорами прав и обязанностей Сторон, содержания расчетных документов и правил заполнения их реквизитов.
  2. ЭД передаются и принимаются Сторонами с использованием Системы ДБО без их последующего представления на бумажном носителе, за исключением случая, предусмотренного п. 4.1.6 настоящих Условий.

1. **ПОРЯДОК ВЕДЕНИЯ РАСЧЕТОВ ЭЛЕКТРОННЫМИ РАСЧЕТНЫМИ ДОКУМЕНТАМИ** 
   1. Списание средств со счета Клиента производится на основании ЭРД Клиента, заверенных ЭП Клиента и переданных им по каналам связи в Банк с использованием Системы ДБО.
   2. После подписания ЭД ЭП внесение каких-либо изменений в поступившие документы, как со стороны Банка, так и со стороны Клиента не допускается.
   3. Списание средств со счета производится в пределах остатка средств по счетам Клиента, указанным в Заявлении на заключение договора о предоставлении услуг с использованием системы ДБО.
   4. ЭРД подписанные ЭП, признаются имеющими равную юридическую силу с другими формами поручений Клиента, подписанными им собственноручно, и могут использоваться в качестве доказательств в суде при возникновении споров.
   5. Порядок подготовки ЭРД, согласованный Сторонами, их формирование, а также порядок обеспечения правильного заполнения форм документов определен в Приложении 1 к настоящим Условиям.
   6. При изменении в карточке с образцами подписей и оттиска печати Клиента состава лиц, уполномоченных распоряжаться счетом, Клиент предоставляет в Банк соответствующие документы, подтверждающие изменения и производит действия для перегенерации ключей и перерегистрации их в Банке.
2. **ПРАВА И ОБЯЗАННОСТИ СТОРОН**
   1. **Банк обязуется:**
      1. Принимать к исполнению поступившие от Клиента подписанные ЭП Клиента ЭРД, оформленные и переданные в Банк в соответствии с настоящими условиями.
      2. Не исполнять ЭРД, поступившие от Клиента, оформленные с нарушением требований действующего законодательства Российской Федерации, нормативных документов Банка России и настоящих Условий, а также при отсутствии или некорректности ЭП Клиента.
      3. Не позднее 5 рабочих дней с даты заключения договора предоставить:

* Клиенту Подсистемы «Интернет-Клиент», логин и пароль, необходимые для работы в Системе ДБО, средство дополнительной защиты для обеспечения безопасности при работе в подсистеме «Интернет-Клиент»[[2]](#footnote-2), ссылку на архив с компонентами ActiveX и архив с инструкциями.
* Клиенту Подсистемы «Банк-Клиент», дистрибутив клиентской части с инструкциями по установке и работе с системой ДБО.
  + 1. По требованию Клиента выдать дополнительные средства защиты:
* USB-ключ eToken PRO (Java) (защищенное хранилище для ключей ЭП );
* Автономный ключ(и) eToken PASS для генерации одноразовых паролей Подсистемы «Интернет-Клиент».
  + 1. Консультировать Клиента по телефону по установке и настройке системы ДБО.
    2. Оформлять и предоставлять Клиенту копии ЭРД с отметкой уполномоченного сотрудника на бумажных носителях, подтверждающие операции, проведенные на основании ЭРД, по отдельному письменному запросу Клиента. Плата за предоставление копий на бумажных носителях взимается согласно п. 8 настоящих Условий.
    3. Обеспечить защиту банковской части Системы ДБО включая содержащуюся в ней ключевую информацию от несанкционированного доступа и сохранять конфиденциальность информации по расчетам Клиента, за исключением случаев, установленных действующим законодательством.
    4. Организовать консультации специалистов Клиента по вопросам проведения расчетов электронными расчетными документами по телефону или, при необходимости, с приездом специалистов Клиента в Банк. Содействовать разрешению вопросов, связанных с особенностью деятельности Системы ДБО в том числе и с привлечением производителя программного обеспечения.
    5. В период действия Договора осуществлять сопровождение установленной у Клиента системы ДБО, как самостоятельно, так и с привлечением сторонних организаций.
    6. Своевременно информировать Клиента об изменениях, касающихся деятельности Банка.
    7. Информировать клиента о каждой операции, совершенной с использованием ЭСП, путем формирования уведомления установленного формата (Приложение 6) не позднее рабочего дня, следующего за днем исполнения распоряжений клиента.
    8. Хранить отправленные клиенту уведомления, log-файлы доступа клиента к системе ДБО не менее 3-х лет.
  1. **Банк имеет право:**
     1. После предварительного предупреждения отказать клиенту в приеме от него распоряжений на проведение операций по счету, подписанных ЭП, в случае возникновения сомнительных операций. При этом право отнесения операций к числу сомнительных принадлежит Банку, на что Клиент дает свое безусловное согласие.
     2. Не принимать к исполнению и не проводить операции по счету Клиента с использованием ЭРД в случаях, установленных п. 7.1. Регламента обслуживания клиентов в Системе ДБО Банка (Приложение 1 к Условиям).
     3. Оформлять от имени Клиента бумажные расчетные документы для передачи в расчетный центр ЦБ РФ на основе полученных Банком по каналам связи электронных расчетных документов (заверять подписями и печатью Банка и проводить соответствующий платеж с указанного в платежном поручении счета Клиента в Банке).
     4. В одностороннем порядке вносить изменения в Систему ДБО, не ухудшающие функциональные возможности и надежность работы указанного программно-технического обеспечения.
     5. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих использованию ЭРД, в одностороннем порядке приостановить на неопределенный срок использование электронных расчетных документов. При этом Банк обязан информировать Клиента, разместив информационное сообщение на сайте банка о возникшем сбое (неисправности) и предполагаемых сроках его устранения. Обмен расчетными документами между Банком и Клиентом в этом случае должен производиться в общем порядке на бумажных носителях.
     6. Контролировать актуальность версий используемого Клиентом программного обеспечения Системы ДБО.
     7. Производить смену используемого в соответствии с настоящими Условиями программно-технического обеспечения с предварительным уведомлением Клиента не менее чем за 7 календарных дней.
     8. Проводить комплекс технических мероприятий по поддержанию системы ДБО в режиме нормальной эксплуатации.
     9. В случае выявления уязвимости в программном обеспечении системы дистанционного банковского обслуживания Банк имеет право, без отдельного уведомления Клиента, внести исправления в программное обеспечение, устраняющие  указанные уязвимости.
     10. В случае получения Банком от банка плательщика (банка - корреспондента) информации о том, что поступившие средства были несанкционированно списаны со счета плательщика, приостановить выдачу/перечисление денежных средств, поступивших на счет Клиента, до выяснения ситуации.
     11. Отключить Клиента от системы ДБО в случаях выявления фактов допуска Клиентом к системе ДБО третьих лиц, а также любого несанкционированного доступа к счету Клиента, до выяснения ситуации.
     12. Временно блокировать доступ Клиента к системе ДБО в случае поступления информации о зачислении на счет Клиента денежных средств, списанных в результате несанкционированного доступа к счетам других клиентов (в том числе в других банках), до выяснения ситуации.
     13. В одностороннем порядке вводить новые, изменять и дополнять действующие Тарифы Банка, порядок и сроки взимания платы, вносить изменения в настоящие Условия, уведомив об этом Клиента не менее чем за 5 рабочих дней до вступления в силу соответствующих изменений, путем публикации информации на Официальном сайте Банка в сети интернет по адресу: [www.baltinvestbank.com](http://www.baltinvestbank.com), и/или путем адресного уведомления Клиента по Системе дистанционного банковского обслуживания (при наличии заключенного Договора дистанционного банковского обслуживания).
     14. По своему усмотрению устанавливать:
* лимиты принимаемых к исполнению с использованием Системы ДБО переводов и платежей по максимальной сумме перевода/платежа и/или по максимальной общей сумме переводов/платежей за заданный Банком период;
* перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием Системы ДБО.
  + 1. Списывать с расчетного счета Клиента, указанного в заявлении на заключение договора комиссию за оказываемые Банком по Договору услуги в соответствии с Тарифами Банка в порядке, предусмотренном п. 8 без распоряжения Клиента (на основании заранее данного акцепта).
  1. **Клиент обязуется:**
     1. Предоставить в Банк Заявление на заключение Договора.
     2. Обес­пе­чить по­ря­док уче­та, хра­не­ния и ис­поль­зо­ва­ния носителей с клю­че­вой ин­фор­ма­ци­ей, ис­клю­чаю­щий не­санк­цио­ни­ро­ван­ный дос­туп к ней по­сто­рон­них лиц.
     3. Строго соблюдать правила эксплуатации Подсистем «Банк-Клиент»\ «Интернет-Клиент», изложенных в их описании и инструкциях по эксплуатации.
     4. Соблюдать требования Регламента Банка по обслуживанию клиентов в Системе ДБО (Приложение 1).
     5. В случае утраты, выхода из строя или компрометации ключей ЭП незамедлительно обратиться в Банк для смены ключей ЭП и принятия необходимых мер (блокирования ключей Клиента в системе электронных расчетов) путем подачи письменного заявления произвольной формы с подробным изложением обстоятельств случившегося (по факсу (812) 326-14-04, по электронной почте [dbo@baltinvest.com](mailto:dbo@baltinvest.com)). Блокировка ключей будет произведена в течение 2-х рабочих часов после поступления заявления в Банк.
     6. В случае необходимости, по письменному запросу Банка предоставить письменное подтверждение факта проведения платежа с использованием электронных форм документов, заверенное подписями уполномоченных лиц, указанных в карточке образцов подписей и оттиска печати.
     7. При уведомлении Банка о смене программного обеспечения принимать меры для своевременного получения и установки новой версии программы.
     8. Не вносить никаких изменений в технические и программные средства Системы ДБО.
     9. Немедленно сообщать Банку письменно обо всех случаях, свидетельствующих о попытках посторонних лиц получить доступ к системе ДБО по факсу 326-14-04, электронной почте [dbo@baltinvest.com](mailto:dbo@baltinvest.com)).
     10. Во всех случаях не подтверждения программной проверкой Системы ДБО ЭП принимаемого ЭРД фиксировать все относящиеся к этому случаю фактические данные и файлы.
     11. После инсталляции Подсистемы «Банк-Клиент» и признания ее работоспособной Клиент принимает на себя ответственность за целостность и неизменность программного обеспечения операционной системы и Подсистемы «Банк-Клиент», установленного на данный ПК.
     12. Обеспечивать на расчетном счете в Банке суммы, необходимые для списания комиссии за ведение счетов с использованием электронного документооборота в соответствии с действующими Тарифами Банка.
     13. Оплачивать услуги Банка в соответствии с Тарифами Банка в порядке, предусмотренном п. 8 настоящих Условий
     14. Указать каналы связи (телефон, факс, e-mail) уполномоченных лиц Клиента для осуществления оперативной связи и своевременно информировать Банк об их изменениях.
     15. Контролировать соответствие суммы платежа остатку средств на своем счете в Банке и осуществлять платежи только в пределах этого остатка.
     16. Не передавать треть­им ли­цам про­грамм­но-технические сред­ст­ва Подсис­те­мы "Банк-Кли­ент" и све­де­ния о при­ме­няе­мой сис­те­ме за­щи­ты ин­фор­ма­ции.
     17. Не устанавливать Подсистему «Банк-Клиент» более чем на один компьютер.
     18. Осуществлять сеансы связи для обмена ЭД не реже 1 раза в 10 календарных дней.
     19. В течение 45 календарных дней с даты заключения Договора подписать в Банке Акт признания ключа проверки электронной подписи.
     20. Читать всю информацию, поступающую из Банка, и руководствоваться ею в дальнейшей работе.
     21. Перегенерировать ключ ЭП не реже одного раза в 15 месяцев с момента регистрации ключа в системе ДБО.
     22. По первому требованию Банка представлять информацию, подтверждающую подлинность (аутентичность) платежного документа, направленного с использованием системы ДБО (в том числе бумажный экземпляр платежного документа, направленного с использованием системы ДБО, с подписями лиц, уполномоченных распоряжаться счетом);
     23. По первому требованию Банка представлять документы, являющиеся основанием для проведения операций по счету Клиента (контракты, договоры, счета, акты и т.д.) во избежание проведения сомнительных операций.
     24. Немедленно сообщать Банку об исключении сотрудника из числа пользователей, которые имеют право доступа в Систему ДБО, в связи с его увольнением, переводом на другой участок работы или по иным причинам, для осуществления замены ключей ЭП.
  2. **Клиент имеет право:**
     1. Заменять ключи ЭП с соответствующим оформлением документов.
     2. Отзывать ЭРД, переданные Банку, в пределах операционного времени в соответствии с условиями Приложения 1. При этом Банк обязан подтвердить факт отзыва ЭРД в течение операционного времени.
     3. При необходимости повторной установки Подсистемы «Банк-Клиент» провести установку своими силами, с уведомлением уполномоченных сотрудников Банка. В этом случае Банк не несет ответственности за работоспособность Подсистемы «Банк-Клиент».
     4. В случае возникновения сбоев в работе Системы ДБО, представлять в Банк расчетные документы для исполнения на бумажных носителях с приложением письма, уведомляющего Банк о факте сбоя и о времени начала предоставления в Банк расчетных документов на бумажных носителях. После устранения возникших сбоев Клиент обязан уведомить Банк произвольным документом Системы ДБО о возобновлении передачи ЭРД.
     5. Взаимодействовать с Банком в ходе расследования факта несанкционированного доступа к счету Клиента, получать от Банка информацию о результатах расследования.
  3. В рамках настоящего Договора Банк осуществляет информационное обслуживание Клиента путем подключения Клиента к сервису «Уведомление об операциях по счету». Порядок предоставления услуги регламентируется Приложением 3 к настоящим Условиям.

1. **БЕЗОПАСНОСТЬ**
   1. Клиент соглашается с получением услуг Системы ДБО, осознавая, что сеть Интернет не является безопасным каналом связи, и соглашается нести все риски, связанные с подключением его вычислительных средств к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет. Стороны также признают, что выход из строя рабочего места Системы ДБО, установленного у Клиента, в результате вмешательства третьих лиц через сеть Интернет, рассматривается как выход из строя по вине Клиента.
   2. Решение об использовании предлагаемых Банком дополнительных сервисов, направленных на повышение безопасности работы системы ДБО, принимается Клиентом самостоятельно.
   3. Банк информирует Клиента об оказываемых дополнительных сервисах, направленных на повышение безопасности работы Клиента в системе ДБО, путем отправки сообщений по системе ДБО, размещением информации на сайте Банка.
2. **ПОРЯДОК РАССМОТРЕНИЯ СПОРНЫХ СИТУАЦИЙ**
   1. При возникновении разногласий Сторон в связи с обменом документов в электронном виде с помощью Системы ДБО, а также в иных случаях возникновения спорных ситуаций в связи с эксплуатацией Системы ДБО, обмен документами в электронном виде с использованием Системы ДБО между сторонами немедленно прекращается.
   2. Сто­ро­ны при­зна­ют, что применяе­мая в Сис­те­ме ДБО ЭП по­зво­ля­ет об­на­ру­жить факт лю­бых из­ме­не­ний в тек­сте ЭД, имею­ще­го ЭП, и обес­пе­чи­ва­ет не­воз­мож­ность под­дел­ки ЭП без знания ключей ЭП.
   3. При раз­ре­ше­нии спор­ных си­туа­ций сто­ро­ны обя­зу­ют­ся ру­ко­во­дство­вать­ся сле­дую­щи­ми прин­ци­па­ми:

* Бремя доказывания лежит на стороне, заявившей о нарушении ее прав и законных интересов.
* Сто­ро­на-получатель обя­зу­ет­ся при­зна­вать под­лин­ным до­ку­мент, пе­ре­дан­ный ей по ка­на­лу свя­зи и имею­щий ЭП, сде­лан­ную на ключах ЭП Стороны-отправителя, при ус­ло­вии по­ло­жи­тель­но­го ре­зуль­та­та про­вер­ки ЭП на со­от­вет­ст­вую­щих ключах проверки ЭП, имеющихся у Стороны-получателя.
* Сторона-отправитель обя­зу­ет­ся при­зна­вать под­лин­ным пе­ре­дан­ный ею до­ку­мент, имею­щий ЭП, сде­лан­ную на ее ключах ЭП, при ус­ло­вии по­ло­жи­тель­но­го ре­зуль­та­та про­вер­ки ЭП на со­от­вет­ст­вую­щих ключах проверки ЭП.
* При получении Стороной-получателем документа с ЭП прошедшей положительную проверку со Стороны-получателя, ответственность возлагается на Сторону-отправителя, так как в этом случае Сторона-отправитель не обеспечила сохранность ключей ЭП.
  1. По инициативе Клиента, если Клиент настаивает на подлинности ЭД, в исполнении которого Банком отказано по причине несоответствия ЭП Клиента содержимому электронного документа, а также в случае неразрешения сторонами спорных ситуаций, назначается Согласительная комиссия для выяснения причин случившегося. Полномочия членов Согласительной комиссии подтверждаются доверенностями. Председатель Согласительной комиссии не избирается, члены Согласительной комиссии равноправны. Если стороны не договорятся об ином, в состав Согласительной комиссии входит равное количество представителей каждой из конфликтующих сторон, но не менее чем по одному уполномоченному представителю. В состав Согласительной комиссии, преимущественно назначаются специалисты из числа сотрудников технических служб, служб информационной безопасности сторон. Лица, входящие в состав Согласительной комиссии, должны обладать необходимыми знаниями в области построения системы криптозащиты, работы компьютерных информационных систем.
  2. По инициативе любой из сторон к работе Согласительной комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, соответствующие требованиям, указанным в п.6.4 настоящего Договора, в том числе разработчики используемых в Системе ДБО средств криптографической защиты информации (СКЗИ). Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.
  3. Каждая из Сторон должна представить согласительной комиссии следующие имеющиеся у нее материалы:
* Ключи проверки ЭП, зарегистрированные в установленном порядке.
* Оспариваемый расчетный документ на бумажном носителе и на электронном носителе в виде файла из Системы ДБО.
  1. Согласительная комиссия производит следующие действия:
* Сравнивает ключи проверки ЭП, предоставленные сторонами. Верным признается экземпляр ключа проверки ЭП, соответствующий «Акту признания ключа проверки электронной подписи (сертификата), хранящемуся в Банке.
* Проверяет подлинность ЭП под спорным документом и наличие его как такового.
* Проверяет log-файлы на компьютерах каждой из Сторон.
  1. Результаты работы согласительной комиссии отражаются в акте, подписываемом всеми членами согласительной комиссии. Члены комиссии, не согласные с выводами большинства, подписывают акт с возражениями, который прилагается к основному акту. Акт составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру акта. По требованию члена комиссии ему может быть выдана заверенная копия акта.
  2. Акт согласительной комиссии является основанием для предъявления требований к лицам, виновным в возникновении конфликта. Претензии к изготовителю Системы ДБО предъявляются Банком. Акт согласительной комиссии может являться доказательством при дальнейшем разбирательстве конфликта в судебных органах.
  3. Порядок определения подлинности ЭД и ЭП, установленный настоящими Условиями, обязателен для Согласительной комиссии.
  4. В случае уклонения какой-либо из Сторон от создания Согласительной комиссии, другие стороны вправе самостоятельно назначить трех независимых экспертов для дачи заключения по вопросу подлинности спорной ЭП. Письменное заключение экспертов составляется в таком количестве экземпляров, чтобы каждая из конфликтующих сторон имела по одному подлинному экземпляру. Заключение экспертов может быть представлено в качестве доказательства в случае разбирательства спора в судебных органах. Расходы по проведению согласительной процедуры возлагаются на сторону, заявившую о нарушении ее прав и законных интересов.

1. **ОТВЕТСТВЕННОСТЬ СТОРОН**
2. Банк и Клиент несут ответственность за достоверность информации, предоставляемой друг другу.
3. Банк не несет ответственности за списание средств со счета Клиента, если Банк до момента проведения платежа не был информирован об обстоятельствах предусмотренных пунктом 4.3.5 Условий.
4. Банк не несет ответственности за двойное списание средств со счета Клиента, в случае одновременного предоставления Клиентом документов с одинаковыми расчетными реквизитами в электронной форме с использованием Системы ДБО и на бумажном носителе.
5. Банк не несет ответственности за полное или частичное неисполнение какого-либо распоряжения Клиента, если это неисполнение явилось следствием форс-мажорных обстоятельств и/или виновных действий третьих лиц.
6. Банк не несет ответственности за допущенную им задержку в оказании услуг, вызванную не предоставлением ЭРД в сроки, оговоренные заключенными Банком и Клиентом договорами банковского счета и договорами на открытие текущего валютного счета, транзитного валютного счета, и расчетно-кассовое обслуживание в иностранной валюте и/или несоответствия расчетных документов установленным требованиям.
7. Банк несет ответственность за сохранность электронных и передаваемых ему бумажных документов и своевременную передачу расчетных документов в банки-корреспонденты.
8. Клиент несет ответственность за правильность оформления электронных расчетных документов.
9. Клиент несет ответственность за сохранность носителя ключей ЭП и за возможные негативные последствия его компрометации, и не вправе предъявлять претензии к Банку по поводу проведенной операции, за исключением случая, когда Клиент предварительно и надлежащим образом уведомил Банк об утрате или компрометации ключей ЭП.
10. Клиент несет ответственность за несвоевременное обновление Подсистемы «Банк-Клиент», которое было передано клиенту на носителе, либо передано посредством Подсистемы «Банк-Клиент».
11. Банк не несет ответственности за качество телефонного соединения с АТС на стороне Клиента.
12. Банк не несет ответственности за работоспособность Интернета на стороне Клиента.
13. Клиент несет всю ответственность за последствия изменений, внесенных в программу или настройки без предварительного согласования с Банком.
14. Банк не несет ответственности за принятие к исполнению подложных и недостоверных документов, если путем простого визуального осмотра (в том числе сверки подписей и оттиска печати (при ее наличии в Карточке) с образцами в банковской карточке), а также в результате контроля подлинности ЭП Банк не мог установить их недостоверность или подложность.
15. Банк возмещает установленные судом потери клиента, имевшие место в результате небрежного исполнения Банком как стороной по Договору своих обязанностей, и в объеме, установленным судебным решением.
16. **СТОИМОСТЬ УСЛУГ И ПОРЯДОК РАСЧЕТОВ**
    1. Плата за услуги Банка по Договору списывается Банком в соответствии с Тарифами Банка со счета Клиента, указанного в заявлении на заключение Договора, без распоряжения Клиента (на основании заранее данного акцепта).
    2. Допускается оплата Клиентом услуг Банка с его расчетных счетов в других банках самостоятельно.
17. **СРОК ДЕЙСТВИЯ ДОГОВОРА И ПОРЯДОК ЕГО РАСТОРЖЕНИЯ**
    1. Срок действия Договора устанавливается с момента подачи Заявления на заключение Договора, в случае положительного результата проверки уполномоченными представителями Банка качества и совместимости технических и программных средств Клиента и действует до 31 декабря текущего года. В случае если ни одна из Сторон письменно не уведомила другую Сторону в срок не позднее, чем за 30 (тридцать) календарных дней до окончания срока действия Договора о своем намерении расторгнуть Договор в одностороннем порядке, действие Договора считается продленным на каждый следующий календарный год.
    2. Договор может быть расторгнут по соглашению Сторон или в одностороннем порядке в случаях, предусмотренных настоящими Условиями.
    3. Банк имеет право расторгнуть Договор в одностороннем порядке без дополнительного уведомления Клиента в случаях:

* если оплата Клиентом услуг по Договору задержана более чем на 10 рабочих дней, действие  Договора прекращается на 15-й рабочий день отсутствия оплаты услуг по Договору;
* если в течение 45 (сорока пяти) календарных дней с даты заключения Договора Клиент не явился в Банк для подписания Акта признания ключа проверки электронной подписи, действие  Договора прекращается на 46-й (сорок шестой) календарный день с даты заключения Договора. При этом средства, списанные Банком со счета Клиента за выезд специалиста и работы по установке и настройке Системы ДБО, Клиенту не возвращаются.
  1. В случае нарушения Клиентом своих обязательств, предусмотренных п.4.3. Условий Банк имеет право в одностороннем порядке расторгнуть Договор путем направления Клиенту соответствующего Уведомления с указанием даты расторжения Договора (за исключением случаев, описанных в п. 9.3. настоящих Условий). Уведомление направляется Клиенту почтой с уведомлением о вручении не менее чем за 5 рабочих дней до даты расторжения Договора.
  2. Действие Договора прекращается также при расторжении договоров банковского счета и/или договоров на открытие текущего валютного счета, транзитного валютного счета и расчетно-кассовое обслуживание в иностранной валюте.
  3. Клиент может досрочно расторгнуть Договор в одностороннем порядке, предварительного письменного уведомив об этом Банк не менее чем за 5 рабочих дней.

1. **ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ**
   1. Все споры между Сторонами разрешаются путем переговоров.
   2. Все споры, связанные с настоящими Условиями, включая споры о действительности Договора в целом или частично, подлежат разрешению в Арбитражном суде по месту заключения договора в соответствии с действующим законодательством.
   3. Все претензии Клиента, связанные с использованием ЭСП, рассматриваются после подачи Клиентом соответствующего заявления в Банк.
2. **ПРОЧИЕ УСЛОВИЯ**
   1. Банк и Клиент осознают и принимают во внимание любые риски, сопутствующие проведению платежей при использовании электронных расчетных документов.
   2. Все приложения, на которые даны ссылки в тексте настоящих условий являются неотъемлемыми частями Договора.
   3. Информация, указанная в Заявлении на заключение договора, изменяется путем оформления корректирующего Заявления на заключение договора и действует с даты его подписания Сторонами.

**Приложение 1**

**к Условиям предоставления**

**услуг с использованием ДБО**

# РЕГЛАМЕНТ

# обслуживания клиентов в Системе Дистанционного банковского обслуживания

# ПАО «БАЛТИНВЕСТБАНК»

1. **Общие положения**

1.1. Банк и Клиент устанавливают между собой порядок ведения счетов с применением электронных расчетных документов в Системе ДБО.

1.2. Электронные расчетные документы, применяемые в Системе ДБО, соответствуют бухгалтерским документам, используемым в соответствии с нормативными актами Центрального Банка Российской Федерации, и являются основанием для осуществления бухгалтерских записей. В случае несоответствия электронного расчетного документа исходному расчетному документу Клиента ответственность за возможный ущерб несет та Сторона, по вине которой возникло указанное несоответствие.

1.3. Для обеспечения безопасности и конфиденциальности расчетов используются специальные процедуры, включающие:

* регистрацию Клиента;
* проверку на наличии электронной подписи;
* проверку электронной подписи ключами проверки электронной подписи;
* формирование формата передачи информации, недоступного к свободному просмотру;
* шифрацию всего информативного трафика, передаваемого Сторонами друг другу.

1.4. Система ДБО обеспечивает выполнение следующих функций:

* подготовка электронных расчетных документов и передача их Банку;
* контроль, обработка и исполнение электронных расчетных документов;
* переписка в свободном формате;
* просмотр/печать принятых из Банка документов;
* просмотр архива.

**2. Организационный порядок проведения расчетов с помощью электронных расчетных документов**

В целях создания организационных предпосылок для осуществления расчетов с помощью расчетных документов в электронной форме:

Банк обязан:

2.1.Не позднее 5 рабочих дней после заключения Договора установить или передать Клиенту программно-технические средства, перечисленные в пунктах 4.1.3, 4.1.4 Договора.

2.2. Зарегистрировать переданные Клиентом ключи ЭП должностных лиц Клиента, уполномоченных распоряжаться счетом, и подписать соответствующие «Акты признания ключа проверки электронной подписи (сертификата)»в двух экземплярах с заверением их мастичной печатью. После этого первый экземпляр передается Клиенту, второй остается в Банке.

Клиент обязан:

2.3. Обладать компьютером типа IBM PC (Celeron 1 ГГц и выше, 1 Гб оперативной памяти) или совместимым с ним, необходимыми программными средствами (Операционная система Windows XP SP3 и выше), необходимыми техническими средствами (принтером, каналом доступа в ИНТЕРНЕТ), располагать квалифицированными кадрами, необходимыми для работы с Банком по Системе ДБО.

В случае использования Подсистемы «Интернет-Клиент» должен быть открыт доступ к IP 91.230.50.100, IP 91.230.50.101, IP 195.5.134.245, IP 195.5.134.247 по 443 порту, на компьютере должен быть установлен Internet Explorer 8.0 и выше.

2.4. После установки Системы ДБО создать ключи ЭП и передать в Банк запросы на перегенерацию ключей. Подписать, распечатанные в Банке в двух экземплярах, «Акты признания ключа проверки электронной подписи (сертификата)»**,** далее - Акты**.** Заверить Акты собственноручной подписью должностных лиц Клиента, уполномоченных распоряжаться счетом, либо подписью доверенного лица Клиента на основании доверенности с проставлением мастичной печати. (При подписании Актов по доверенности мастичная печать не проставляется.)

2.5. В случае невозможности установки Подсистемы «Банк-Клиент» на предоставленный компьютер (программная или аппаратная несовместимость) предоставить другой компьютер для установки данного программного обеспечения.

2.6. **Не устанавливать Подсистему «Банк-Клиент» более чем на один компьютер**.

**3. Порядок использования расчетных документов, подписанных ЭП**

3.1.Совершение сделок в письменной форме с использованием ЭП регулируется ст.160 Гражданского кодекса Российской Федерации.

3.2. ЭП удостоверяет факт подлинности, целостности и подписания расчетного документа от имени Клиента для целей его обработки с помощью вычислительной техники.

3.3. Право использовать ключ ЭП Клиентом возникает с момента регистрации уполномоченным сотрудником Банка средств проверки правильности ЭП (ключа ЭП) Клиента.

3.4. Ключ ЭП хранится в виде файлов на дискете (3,5”), флэш-памяти, ином отчуждаемом носителе, именуемой в дальнейшем «носитель ключа ЭП», и используется Клиентом в целях запуска процесса подписания электронной подписью документов, подготовленных с помощью средств вычислительной техники или расшифрования полученных по Системе ДБО документов.

3.5. Достоверность расчетного документа, подписанного ЭП и направленного в Банк, считается подтвержденной, если выполнение Банком установленных процедур проверки ЭП дает положительный результат.

3.6. Результаты проверки должны фиксироваться в специальном журнале с использованием электронных средств.

3.7. Расчетный документ, подписанный ЭП, передается Банку способом, обеспечивающим сохранение всех обязательных реквизитов расчетного документа.

3.8. Расчетный документ, подписанный ЭП, воспроизводится на бумажном носителе с сохранением всех реквизитов расчетного документа.

**4. Подготовка Клиентом электронных расчетных документов и передача их в Банк**

4.1. Клиент представляет в Банк электронные расчетные документы, подготовленные по установленной форме. При этом он выводит на экран ПЭВМ средствами Подсистемы «Банк-Клиент»\ «Интернет-Клиент» электронную форму документа и заполняет в ней реквизиты согласно наименованиям полей.

4.2. Документы должны содержать электронные отметки о результатах обработки. Отметки должны соответствовать требованиям технической документации, передаваемой Клиенту Банком.

4.3. Передача документов в Банк осуществляется с помощью подсистемы коммуникаций, которая запускается из оболочки Подсистемы «Банк-Клиент», или через интернет – браузер а случае использования Подсистемы «Интернет-Клиент».

4.4. Платеж считается принятым к исполнению только при получении Клиентом электронной квитанции согласно п.п. 5.2. и 5.3. настоящего Регламента

**5. Контроль, обработка и исполнение электронных расчетных документов Банком.**

5.1. Автоматический контроль правильности заполнения электронных расчетных документов осуществляется в два этапа – на этапе заполнения документа Клиентом и на этапе приема документов компьютером Банка.

5.2. При поступлении документов в Банк производятся следующие действия:

* расшифровка, проверка ЭП;
* сохранение пакета в контрольном архиве;
* внутренняя проверка реквизитов документов;
* передача документов в обработку в Подсистему «Банк».

По итогам проведенных процедур документу присваивается статус «Принят» и формируется электронная квитанция Клиенту, изменяющая статус документа в Подсистеме «Банк-Клиент» на «Принят». Статус «Принят» означает, что документ доставлен в Банк, прошел расшифровку и проверку ЭП, но еще не был рассмотрен уполномоченными сотрудниками Банка (см. п.5.3). Для получения электронной квитанции с информацией о прохождении документа Клиент должен установить повторный сеанс связи не ранее, чем через 15 минут после успешного сеанса по передаче электронных расчетных документов в Банк. При использовании Подсистемы «Интернет-Клиент» необходимо убедиться в перемещении документа в группу «В обработке» со статусом «Принят». В случае неполучения электронной квитанции о статусе документа, а так же при получении статусов «Ошибка подписи», «Отказан АБС», «Не принят» и т.д., Клиент обязан связаться с уполномоченными сотрудниками Банка для выяснения причин, вызвавших задержку в получении квитанции или ошибку.

5.3. Обработка документов в Банке осуществляется уполномоченными сотрудниками Банка. По результатам обработки документов документ может быть принят к исполнению или не принят к исполнению.

**6. Временной режим.**

6.1. Активной Стороной при установлении связи и в процессе приема – передачи сообщений является Клиент.

6.2. Режим работы Системы ДБО с 06-00 до 00-00 по Московскому времени.

6.3. Принятые от Клиента пакеты документов и запросы проходят обработку компьютером Банка.

Документы, переданные Клиентом, обрабатываются и проводятся в сроки, определенные заключенным между Банком и Клиентом Договором банковского счета.

6.4. Клиент имеет право отозвать переданные электронные расчетные документы. Документ подлежит отзыву (отказу от исполнения) при условии, что он не передан для дальнейшей обработки в МЦИ ЦБ РФ. При необходимости отзыва документов Клиент обязан: связаться с уполномоченными сотрудниками Банка, выяснить текущий этап обработки документа и, при возможности отзыва, уведомить уполномоченного сотрудника Банка о намерении отозвать документ;

* в течение 10 минут после уведомления уполномоченного сотрудника Банка подготовить и отправить через Систему ДБО в Банк письмо (в Системе ДБО реализован как «Произвольный документ») с просьбой отозвать электронный расчетный документ с точным указанием даты, номера, суммы и реквизитов получателя отзываемого электронного расчетного документа.

**7. Отказ от исполнения электронных документов.**

7.1. Основанием для отказа Банка от исполнения электронного расчетного документа служит:

* несоответствие электронной подписи содержащейся в документе;
* **компрометация ключей ЭП, о которой стало известно Банку;**
* неверно указанные платежные реквизиты или их отсутствие;
* несвоевременная оплата услуг Банка по Системе ДБО;
* несоответствие содержания документа другим установленным требованиям.

**Приложение 2**

**к Условиям предоставления**

**услуг с использованием ДБО**

**Памятка по обеспечению безопасности при работе в системе Дистанционного Банковского Обслуживания (ДБО) «Интернет-Клиент» и «Банк-Клиент»**

***Банк считает критически важным выполнение Клиентами  
следующих основных рекомендаций:***

* ***Использовать дополнительные решения в сфере обеспечения безопасности при работе в системе «Интернет-Клиент» и «Банк-Клиент», предлагаемые Банком (средства дополнительной защиты): сеансовые ключи, USB-ключи, МАС-фильтраця,* *SMS-авторизация***2***.***
* ***Обеспечить безопасность ключа ЭП и носителей с ключами ЭП.***
* ***Соблюдать регламент ограниченного доступа к компьютеру.***
* ***Использовать Лицензионное программное обеспечение (ПО).***
* ***Использовать и оперативно обновлять системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ.***
* ***Использовать и оперативно обновлять специализированное ПО для защиты информации – антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.***
* ***Соблюдать правила безопасной работы в интернете.***

**1. Использование дополнительных решений в сфере обеспечения безопасности при работе в Подсистеме «Интернет-Клиент», предлагаемые Банком (USB-кючи, МАС-фильтрация, сеансовые ключи, SMS-авторизация**2**).**

**MAC-фильтрация**

В целях повышения безопасности клиент может использовать услугу “MAC-фильтрация”. Данный механизм позволяет исключить возможность работы в системе ДБО всех компьютеров, кроме тех, чьи MAC-адреса официально предоставлены Банку. МАС -фильтрацию можно успешно применять, даже если рабочее место клиента не обладает статическим (неизменным) IP-адресом в Интернете. При попытке входа в систему с другого компьютера, чей MAC-адрес отличается от официально указанного клиентом Банку, система проинформирует о невозможности соединения с Банком, даже если при попытке выхода в систему будет использован зарегистрированный ключ.

**Использование MAC-фильтрации с одной стороны ограничит возможности клиента работать, используя подключение к Интернет в произвольном месте, но с другой серьезно затруднит использование злоумышленником похищенного ключа ЭП клиента.**

**Использование сеансовых ключей**

Для дополнительной аутентификации Банк предлагает использовать автономный генератор одноразовых паролей **eToken PASS**. Одноразовый пароль действует только в течение одного сеанса связи – пользователь может не беспокоиться о том, что пароль может быть подсмотрен и перехвачен. Гарантируемый срок службы – 7 лет или 14 000 генераций.

**SMS-авторизация[[3]](#footnote-3)**

В целях снижения рисков, связанных с работой в сети Интернет,  Банк  может установить уполномоченным лицам Клиента признак, обеспечивающий их вход в Интернет-Клиент после ввода одноразового пароля, направляемого Банком на мобильный телефон Уполномоченного лица Клиента (SMS авторизация). Одноразовый пароль действует только в течение одного сеанса связи. Время, в течение которого осуществляется доставка кода с помощью SMS, зависит от оператора мобильной связи и местоположения абонента.

**2.Обеспечение безопасности ключа ЭП и носителей с ключами ЭП.**

**Для хранения ключей ЭП использовать только внешние носители (дискеты или флеш-накопители, токены), а не жёсткие/сетевые диски компьютера. Владелец ключа ЭП должен хранить его в условиях, исключающих доступ к нему третьих лиц** (Хранить при себе или использовать для хранения личный сейф). **Нельзя** записывать пароли на листах бумаги, приклеенных к дисплею рабочего компьютера. **В случае потери ключа ЭП или утраты пароля, необходимо немедленно сообщить об этом в банк любым доступным способом.** Только после этого доступ к системе будет заблокирован и злоумышленник не сможет воспользоваться вашим счетом в Банке!

**Нельзя использовать носители с ключами ЭП для каких-либо других целей** (в частности, не хранить на них любую другую информацию). **Необходимо извлекать носители с ключами ЭП из компьютера каждый раз после завершения их использования** (т.е. носители с ключами ЭП должны находиться в компьютере только в период подписания документов).

Стоит обратить внимание, что чаще всего хищение ключей возможно в следующих случаях:

С использованием сети Интернет в результате заражения компьютера вредоносным ПО (вирусами, троянами и т.д.), с помощью которого злоумышленники производят хищение ключей ЭП и паролей.

Бывшими сотрудниками компании, имевшими доступ к ключам либо к системе «Интернет-Клиент», IТ-специалистами (штатными и внештатными), привлекаемыми из сторонних организаций для оказания различных услуг (обновление различных программ компании, например, бухгалтерских, подключение к Интернет и т.д.)

**Необходимо производить смену пароля и производить перерегистрацию ключей ЭП при возникновении подозрений о компрометации ключей/паролей на доступ к системе, а так же при увольнении сотрудника, имевшего доступ к ключам и системе ДБО.**

**Защита ключа ЭП от хищения**

**Одним из наиболее надежных средств защиты ключа ЭП от хищения злоумышленниками является использование защищенного хранилища в виде смарт-карты. Наш Банк предлагает такое решение в виде USB-ключа “eToken” от фирмы Aladdin**

**Использование USB-ключа «eToken» на данный момент является действенной мерой, предотвращающей хищение (копирование) троянами и злоумышленниками ключей ЭП клиентов.**

**3. Соблюдение регламента ограниченного доступа к компьютеру**

Следует строго соблюдать регламент ограниченного доступа к компьютеру, используемому для работы с системой ДБО.

Любой физический доступ к компьютеру – это потенциальная возможность подключения отчуждаемого носителя (дискеты, компакт-диска, USB-накопителя) и, как следствие, возможность привнесения на компьютер вредоносной программы (вируса, трояна и т.п.).

Любой физический доступ к компьютеру – это потенциально неконтролируемая работа в Интернете, и, как следствие, возможность случайной или намеренной загрузки вредоносной программы. Поэтому Банк рекомендует придерживаться следующих правил, позволяющих обеспечить контролируемый физический доступ к компьютеру, с которого осуществляется работа по системе ДБО**.**

* Право доступа к рабочим местам, с которых осуществляется работа с ПО системы ДБО должно предоставляться лицам, непосредственно осуществляющим работу с системой ДБО и иным лицам в соответствии с внутренним регламентом организации.
* Доступ посторонних лиц в помещения с рабочими местами системы ДБО должен осуществляться под контролем сотрудника службы безопасности организации.
* Не следует оставлять без контроля рабочие места системы ДБО. При кратковременном отсутствии необходимо: сохранить все открытые на редактирование документы; средствами операционной системы заблокировать рабочее место.
* Для исключения возможности несанкционированного изменения аппаратной части системный блок и разъемы рабочих мест системы ДБО должны опечатываться сотрудником службы безопасности организации и, при каждом включении должна проверяться их целостность.
* На рабочих местах системы ДБОследует использовать только лицензионное программное обеспечение.
* На рабочих местах системы ДБОдолжны быть отключены: загрузка с гибкого диска, загрузка по сети, если внутренним регламентом организации не предусмотрено иное.
* Вход в BIOS рабочих мест системы ДБО должен быть защищен паролем. Пароль для входа в BIOS должен быть известен только системному администратору или другому лицу в соответствии с внутренним регламентом организации.
* Для всех учетных записей в операционной системе должны использоваться пароли, удовлетворяющие следующим требованиям: длина пароля не менее 6 символов; в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы; периодичность смены пароля определяется политикой безопасности организации, но не должна превышать одного года.
* Количество неудачных попыток входов в систему должно быть ограничено в соответствии с политикой безопасности, принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток.
* Должна быть отключена учетная запись для гостевого входа (Guest).
* Должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке.
* Должны быть отключены режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей .
* В случае обнаружения на рабочих местах системы ДБО незарегистрированных программ, нарушения целостности операционной системы, либо выявления факта повреждения печатей на системных блоках, работа должна быть прекращена.
* Для защиты от несанкционированного доступа к рабочим местам системы ДБО из внешней сети рекомендуется использовать антивирусное ПО и персональный межсетевой экран.

**4. Использование и обновление системного и прикладного ПО**

Установка и обновление системного и прикладного ПО (операционная система, браузеры, почтовые клиенты, офисные программы, бухгалтерские программы и пр.) из ненадежных источников приводит к проникновению на компьютер клиента вредоносных программ, в том числе троянов. **Следует использовать программное обеспечение только из надежных доверенных источников.**

Если это коммерческие программы – Microsoft Windows, Microsoft Office, 1С:Бухгалтерия и пр. – они должны быть легально приобретены клиентом и установлены с легального дистрибутива, гарантирующего отсутствие вредоносных программ. Если это свободно распространяемые программы – Linux, Firefox, Thunderbird, Java и пр. – они должны быть получены на компакт-диске из доверенного источника или загружены через Интернет с публичных сайтов разработчиков с использованием механизмов обеспечения целостности загружаемого ПО. Данные меры предосторожности также применимы и при получении на носителях или загрузке из Интернета обновлений используемого системного и прикладного ПО. При этом необходимо строго придерживаться рекомендаций разработчиков о периодичности проверки появления новых версий и обновлений программного обеспечения.

**Оперативное обновление системного и прикладного ПО на компьютере клиента – это необходимое условие для снижения рисков заражения компьютера вредоносными программами, в том числе троянами через новые выявленные уязвимости и ошибки в используемых клиентом программах.**

**5. Использование и обновление ПО для защиты информации**

Для защиты от вредоносных программ в первую очередь необходимо использовать и оперативно обновлять на своем компьютере специализированные программы для защиты информации:

Антивирусное ПО;

Персональные межсетевые экраны;

Средства защиты от несанкционированного доступа.

В настоящее время пользователям доступно достаточное количество специализированных программных средств защиты информации – как коммерческих, так и свободно распространяемых.

**Минимально необходимый набор на компьютере клиента – это антивирусное ПО + персональный межсетевой экран (firewall).**

**6. Соблюдение правил безопасной работы в сети Интернет.**

**Рекомендации пользователям Подсистемы «Интернет-Клиент»**

**Наиболее надежным способом обеспечения безопасности данных клиента при работе в системе «Интернет-Клиент» является использование компьютера только для работы с указанной системой и исключение случаев использования применяемого компьютера для каких-либо других задач.**

Вне зависимости от того, используется ли компьютер, применяемый для работы в системе «Интернет-Клиент» для каких-либо иных целей, мы рекомендуем клиентам неукоснительное соблюдение следующих правил безопасности:

* Никогда не открывать сайт Подсистемы «Интернет-Клиент» по ссылкам (особенно баннерным или полученным через почту), поскольку существует множество способов фальсифицировать адрес. Необходимо всегда самостоятельно вводить в адресной строке Web-браузера с обязательным указанием используемого протокола [https://iclients.baltinvest.ru](https://iclients.baltinvest.ru/) или через корпоративный сайт Банка.
* Не отвечать ни на какие обращения с просьбой выслать ключ проверки ЭП, пароль и другие конфиденциальные данные (Телефонные звонки от якобы представителей банка, письма по электронной почте, SMS и т. п.) Подобные запросы наверняка производятся злоумышленниками. Сотрудники БАНКА ни при каких обстоятельствах **не могут запрашивать у клиентов эти конфиденциальные данные.**
* Обращать особое внимание на отправителя почтовой корреспонденции при работе с электронной почтой, вне зависимости от того, выполняется работа с почтой через Web-интерфейс одной из известных почтовых систем mail.ru, yandex.ru и т.п., или в локально установленных программах типа Outlook, Outlook Express, The Bat! Не открывать вложение письма, что бы ни содержало данное сообщение, если отправитель почтового сообщения вам неизвестен. Обратить внимание: никакие обновления, патчи, апдейты для компьютеров не распространяются по почте. При переписке со всеми адресатами необходимо помнить, что даже в письме известного клиенту отправителя, в том числе отправителя, с которым ведется длительная переписка, может находиться вредоносное вложение. Открывать вложения, полученные по электронной почте, необходимо только после предварительного сохранения их в специальной папке на жестком диске и проверки их на наличие вредоносных программ (антивирусной проверки).
* При использовании служб мгновенного обмена сообщениями – ICQ, Instant Messaging, Mail.ru-агент и т.д. необходимо соблюдать рекомендации аналогично работе с почтовыми клиентами – не принимать файлы из неизвестных источников, к файлам из известных источников относиться с осторожностью**. Проверять все полученные файлы антивирусными программами**.
* Не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять, а в случае необходимости загрузки такого файла следует убедиться, что он проверен антивирусом.
* Не допускать использования компьютера для посещения сайтов сомнительного содержания (сайты эротической направленности, сайты бесплатных программ, хакерские сайты и т.п.). Зачастую такие сайты содержат вредоносные программы, загружаемые и запускаемые при входе на сайт.
* Немедленно вызывать системного администратора при любом подозрении, заражения компьютера (неадекватная реакция на действия пользователя, самостоятельная активность, появляющиеся непонятные окна и т.п.).

**ПРЕДУПРЕЖДЕНИЕ.**

В Интернете есть специализированная вредоносная программа (троян), которая похищает у пользователей Подсистемы «Интернет-Клиент» файлы с ключами ЭП и пароли, вводимые с клавиатуры.

Троянская программа, проникнув на компьютер клиента, используя уязвимость системного программного обеспечения, перехватывает управление, подменяет системные динамические библиотеки, после чего начинает отслеживать ввод с клавиатуры, файловый ввод-вывод с поиском файлов с ключами ЭП клиента, сетевой ввод-вывод, а также вызовы динамических библиотек.

Во время блокирования компьютера клиента злоумышленники, используя похищенный ключ ЭП и пароль, подключаются банковскому серверу и от имени клиента отправляют в банк платежное поручение с корректной ЭП клиента. При этом вся ответственность за убытки безусловно и полностью возлагается на клиента как единственного владельца ключей ЭП.

За последние несколько месяцев в ряде российских банков выявлены случаи хищения средств с расчетных счетов организаций, с использованием ранее похищенных ключей ЭП этих организаций. Впоследствии на компьютерах ответственных сотрудников данных организаций и был обнаружен вышеуказанный троян.

Детальный анализ работы выявленного трояна показывает, что злоумышленники эксплуатируют фундаментальную проблему – **неспособность некоторых пользователей обеспечивать доверенную среду на своем компьютере**.

Если ваш компьютер вышел из строя (не загружается система) и вы не можете связаться с банком по системе ИНТЕРНЕТ-клиент - обязательно сообщите об этом факте в службу поддержки БАНКА.

**За дополнительной информацией, а так же по всем вопросам эксплуатации системы ДБО обращайтесь в ПАО «БАЛТИНВЕСТБАНК» по телефонам:**

**(812) 326-14-18**

**Приложение 3**

**к Условиям предоставления**

**услуг с использованием ДБО**

1. **Порядок предоставления сервиса «Уведомление об операциях по счету»**
   1. Услуга «Уведомление об операциях по счету» предоставляется при условии использования системы ДБО.
   2. Банк и Клиент подтверждают свое согласие на оказание услуг посредством передачи Клиенту SMS-сообщений на номер телефона, указанный в Заявлении при наступлении событий, отмеченных в п. 1.3, 1.4 , 1.5 настоящего Приложения.

При заключении Договора Клиенту предоставляется базовый пакет подключения услуги «Уведомление об операциях по счету». Подключение дополнительных опций осуществляется на основании заявки.

* 1. Клиент, оформляя заявку на подключение дополнительных опций сервиса, безусловно соглашается с получением от Банка SMS-сообщений, содержащих информацию в объеме, установленном в Перечне доступных опций, а так же входящим в базовый пакет подключения.
  2. К событиям, доступным через сервис «Уведомление об операциях по счету», входящим в базовый пакет подключения, относится «Вход в систему «Интернет-Клиент», «Вход в систему «Банк-Клиент».
  3. Банк обязан направлять Клиенту SMS-сообщения при наступлении события, указанного в п. 1.3, а также выбранного Клиентом в Перечне доступных опций через сервис «Уведомление об операциях по счету».
  4. Банк оставляет за собой право вносить изменения в режим работы сервиса «Уведомление об операциях по счету», в перечень событий и форматов SMS-сообщений, предварительно уведомив об этом Клиента за 5 рабочих дней.
  5. Банк имеет право в одностороннем порядке временно приостановить оказание услуг Клиенту в рамках Договора и блокировать доступ к сервису «Уведомление об операциях по счету» без предварительного уведомления Клиента, если, по мнению Банка, такая мера необходима для обеспечения безопасности системы. Приостановление оказания услуг в соответствии с настоящим пунктом не является основанием для возврата Клиенту денежных средств.
  6. Клиент предоставляет Банку безусловное право на направление в адрес Клиента SMS-сообщений информационного и рекламного характера.
  7. В случае утраты Клиентом мобильного телефона или SIM-карты Клиент обязуется не предъявлять требований, а Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну Клиента или персональные данные Клиента либо сотрудников клиента.
  8. В случае утраты мобильного телефона или SIM-карты с номерами телефонов, указанных в Заявке, Клиент обязан незамедлительно уведомить об этом Банк для отключения номера телефона от сервиса «Уведомление об операциях по счету».
  9. 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-сообщений Клиенту.
  10. Клиент уведомлен и согласен с тем, что используемые для передачи SMS-сообщений, телекоммуникации являются открытыми и не гарантируют полную защиту информации, передаваемой в рамках Договора. Клиент согласен с тем, что Банк не несет ответственности за возможное раскрытие информации, составляющей банковскую тайну.
  11. Любые дополнительные расходы и издержки, понесенные Банком при обслуживании Клиента с использованием сервиса «Уведомление об операциях по счету» Банка и не предусмотренные договором и Тарифами Банка, оплачиваются Клиентом отдельно на основании отдельных Договоров или Дополнительных соглашений.
  12. Клиент самостоятельно оплачивает услуги других организаций, привлечение которых необходимо для нормального функционирования его системы получения SMS-сообщений с сервисом «Уведомление об операциях по счету», а также за собственный счет поддерживает в надлежащем состоянии свои помещения, технические и аппаратные средства.

1. **Перечень доступных опций через сервис «Уведомление об операциях по счету»**

|  |  |  |
| --- | --- | --- |
| **Подсистема «Интернет-клиент»** |  | **Подсистема «Банк-Клиент»** |
| Изменение пароля пользователя |  |
| Учетная запись заблокирована |
| П/п принято | П/п принято |
| П/п исполнено | П/п исполнено |
| Поручение на покупку/продажу валюты принято |  | Поручение на покупку/продажу валюты принято |
| Поручение на покупку/продажу валюты исполнено |  | Поручение на покупку/продажу валюты исполнено |
| Поручение на перевод валюты принято |  | Поручение на перевод валюты принято |
| Поручение на перевод валюты исполнено |  | Поручение на перевод валюты исполнено |

**Приложение 4**

**к Условиям предоставления**

**услуг с использованием ДБО**

**Рекомендации по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

В связи с участившимися случаями хищения денежных средств в системах дистанционного банковского обслуживания, использующих электронные устройства (персональный компьютер, iPad, ноутбук и т.п.) клиента (далее - ДБО), в соответствии с письмом Ассоциации российских банков и Некоммерческого партнерства "Национальный платежный совет" от 20 июля 2012 г. NN А-02/1А-424, НПС-02/1-89 "О применении рекомендаций о действиях в связи с совершением мошенничества в системах ДБО", разработаны следующие  **рекомендации**

**Порядок действий в случае выявления хищения денежных средств**

1. В случае выявления хищения денежных средств в системе ДБО немедленно прекратить любые действия с электронным устройством (ЭУ), подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь аккумуляторную батарею из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi и др.) или перевести в режим гибернации.

2. При наличии технической возможности отозвать перевод с использованием иного ЭУ, после чего заблокировать систему ДБО.

3. При отсутствии технической возможности отозвать перевод по системе ДБО немедленно обратиться в банк **по телефону/факсу (326-14-04)**  с заявлением о приостановке исполнения платежа и возврате средств.

4. Произвести фотосъёмку 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 опечатать горловину. При необходимости ведения хозяйственной деятельности - задействовать другое ЭУ.

5. Обратиться в банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе ДБО. (Приложение I к настоящим Рекомендациям), а также о компрометации ключей и необходимости смены пароля (закрытого ключа). Копия заявления должна быть направлена в банк плательщика незамедлительно по факсу (326-14-04) или по электронной почте (скан-копия)([dbo@baltinvest.com](mailto:dbo@baltinvest.com)). Оригинал заявления должен быть доставлен в банк плательщика в течение одного дня.

6. Проинформировать все банки, с которыми имеются договорные отношения, предусматривающие использование ДБО, о факте хищения денежных средств и обратиться с просьбой о внеплановой замене ключевой информации.

7. В течение одного дня обратиться в банк получателя или к оператору соответствующей платежной системы с письменным заявлением о приостановлении платежа и возврате денежных средств (Приложение II к настоящим Рекомендациям).

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.

9. Провести сбор записей с межсетевых экранов, серверов баз данных и иных компонент клиентского приложения системы ДБО, систем авторизации пользователей (AD, NDS и т.д.), ЭУ, используемых для управления денежными средствами через систему ДБО банка, устройств, которые могут использоваться для удалённого управления указанными ЭУ.

10. В течение одного дня обратиться с письменным заявлением к своему Интернет-провайдеру (Приложение III  к настоящим Рекомендациям) для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его ЛВС как минимум за три месяца, предшествовавшие факту хищения денежных средств.

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 ИТ для восстановления работоспособности.

12. Зафиксировать в протокольной форме значимые действия и события, в том числе действия с ЭУ, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения клиента (работников клиента) об использовании ЭУ в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе ЭУ, перебоях или отказах ЭУ, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших в месте расположения ЭУ и т.д.

13. Все действия, указанные в пп. 1, 4, 8, 9, 12 , производить коллегиально, протоколировать и документировать, в т.ч. с использованием фотосъёмки.

14. В течение одного дня обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по факту хищения денежных средств (Приложение IV к настоящим Рекомендациям).

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 КУСП, содержащую отметку правоохранительного органа о его приеме.

16. Копии вышеуказанных документов по перечню, направить в банк плательщика с приложением Справки по факту инцидента информационной безопасности в системе ДБО (Приложение V) настоящим Рекомендациям), а также подтверждающих документов (Приложение VI) к настоящим Рекомендациям)

**Приложение I к Рекомендациям по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**ЗАЯВЛЕНИЕ ПЛАТЕЛЬЩИКА В БАНК ПЛАТЕЛЬЩИКА ОБ**

**ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И**

**БЛОКИРОВАНИИ ДОСТУПА К СИСТЕМЕ ДБО**

В ПАО «БАЛТИНВЕСТБАНК»

От\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование организации

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ года с нашего расчетного счета №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,открытого в ПАО «БАЛТИНВЕСТБАНК», по системе дистанционного банковского обслуживания были похищены денежные средства, которые, по имеющейся информации были переведены со следующими реквизитами платежа:

Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Номер платежного поручения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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 заблокировать нашу учетную запись в системе ДБО, провести процедуру компрометации всех ключей ЭП и оказать содействие в возврате денежных средств.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность подпись расшифровка подписи

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

Исп. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение II к Рекомендациям по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА В БАНК ПОЛУЧАТЕЛЯ ИЛИ К**

**ОПЕРАТОРУ ПЛАТЕЖНОЙ СИСТЕМЫ О ПРИОСТАНОВЛЕНИИ ПЛАТЕЖА**

**И ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность руководителя

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

Уважаемый (ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

имя, отчество руководителя

    "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года с нашего расчетного счета

были похищены денежные средства, которые, по информации, полученной из

банка, были переведены со следующим реквизитам платежа:

    Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер платежного поручения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[\*](#sub_2111)

    Прошу Вас оказать содействие в приостановлении прохождения платежа и

возврате денежных средств.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность подпись расшифровка подписи

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_

Исп. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение III к Рекомендациям по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**ФОРМА ПИСЬМА ИНТЕРНЕТ ПРОВАЙДЕРУ О ПРЕДОСТАВЛЕНИИ**

**ЖУРНАЛОВ СОЕДИНЕНИЙ (ЛОГОВ)**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность руководителя

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование организации

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность, ФИО заявителя

проживающего: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

адрес места жительства

паспорт: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

номер паспорта, дата выдачи, кем и когда выдан

контактный телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

телефон заявителя

адрес для корреспонденции \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

почтовый адрес

Уважаемый (ая) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

имя, отчество руководителя

    "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ года в \_\_\_:\_\_\_ по московскому

времени со счета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ по системе дистанционного

банковского обслуживания (ДБО) был осуществлен несанкционированный

перевод денежных средств. Компьютер, с которого осуществляется

подключение к системе ДБО, располагается по адресу

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и использует IP-адрес \_\_\_.\_\_\_.\_\_\_.\_\_\_.

    Вероятной причиной несанкционированного перевода могло послужить

заражение компьютера вредоносным программным обеспечением, кража логина,

пароля и секретных ключей системы ДБО.

    "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ года между \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и вами был

заключен договор N \_\_\_\_\_\_ об оказании \_\_\_\_\_\_\_\_\_\_\_\_\_ услуг.

Для выявления обстоятельств несанкционированного перевода 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\_\_

Исп. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия И.О.

тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение IV к Рекомендациям и по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) В**

**ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ О ВОЗБУЖДЕНИИ УГОЛОВНОГО**

**ДЕЛА ПО ФАКТУ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ**

Начальнику ОВД по \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование ОВД

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

должность, ФИО заявителя

проживающего: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

адрес места жительства

паспорт: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

номер паспорта, дата выдачи, кем и когда выдан

место работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование организации

контактный телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

телефон заявителя

адрес для корреспонденции \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

почтовый адрес

**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) "\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"

наименование банка

    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г. неизвестными лицами по системе ДБО был

осуществлен несанкционированный перевод денежных средств со следующими

реквизитами:

    Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер платежного поручения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[\*](#sub_4111).

    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 появления этого перевода был установлен "\_\_" \_\_\_\_\_\_\_\_\_ 201\_\_ г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ФИО лица, установившего факт несанкционированного перевода, должность,

наименование организации

при \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

обстоятельства обнаружения факта несанкционированного перевода

    Электронное устройство, с которого осуществляется подключение к

системе ДБО, располагается по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, доступ к

электронному устройству ограничен, прямая кража реквизитов доступа

(учетной записи, пароля и секретных ключей) маловероятна.

    Вероятной причиной этого несанкционированного перевода 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\_\_ г.

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /               /

подпись

**Приложение V Рекомендациям и по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ**

**БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО**

    "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ неустановленным лицом через систему ДБО была совершена несанкционированная операция по переводу денежных средств

со следующими реквизитами:

    Дата платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер платежного поручения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета плательщика: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование банка получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Наименование получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    ИНН получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Номер счета получателя: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Сумма платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

    Назначение платежа: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[\*](#sub_5111)

    Дополнительно сообщаю:

Количество ЭУ, настроенных для доступа в систему ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Для доступа в системы ДБО хотя бы раз использовались

┌─┐

   │ │корпоративные ЭУ

└─┘

┌─┐

   │ │личные ЭУ

└─┘

┌─┐

   │ │ЭУ, находящиеся в общественном пользовании

└─┘

Периодичность смены пароля системы ДБО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Применяемые элементы безопасности ЭУ включают:

┌─┐

   │ │соблюден порядок подготовки ЭУ к установке системы ДБО

└─┘

┌─┐

   │ │используется только программное обеспечение для работы системы ДБО

└─┘

┌─┐

   │ │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

└─┘ключевые носители

┌─┐

   │ │передача файлов и обмен сообщениями электронной почты на ЭУ

└─┘ограничены

┌─┐

   │ │целостность исполняемых файлов и файлов конфигураций

└─┘ контролируется с периодичностью \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

┌─┐

   │ │используются средства сетевой защиты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

└─┘

┌─┐

   │ │на ЭУ запрещены входящие соединения из сети Интернет

└─┘

┌─┐

   │ │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 ключевым носителям только

└─┘ уполномоченных лиц

Иная информация, имеющая отношение к инциденту: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Подтверждаю отсутствие у меня претензий к \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

наименование банка плательщика

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

подпись плательщика

┌─┐

│ │Я намерен обратиться в правоохранительные органы по факту хищения

└─┘денежных средств.

Заявление в правоохранительные органы принято в ОВД \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

район, округ, город, субъект федерации и иные идентифицирующие ОВД

данные

и зарегистрировано за N \_\_\_\_\_\_ в КУСП

┌─┐

│ │Я не намерен обращаться в правоохранительные органы по факту хищения

└─┘денежных средств.

О необходимости предоставления доступа сотрудников правоохранительных

органов к электронному устройству, об ответственности за использование

нелицензированного и контрафактного программного обеспечения в

соответствии со [статьей 146](garantF1://10008000.146) УК Российской Федерации предупрежден.

Заявитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Дата: \_\_\_\_\_\_\_\_\_\_\_\_\_\_/Телефон: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Приложение VI Рекомендациям по порядку действий в случае выявления факта хищения денежных средств со счета Клиента**

**Примерный перечень  
документов, которые могут быть истребованы у плательщика в случае выявления хищения денежных средств**

1. Копия лицензии на операционную систему ПК.

2. Копия чека на приобретение операционной системы ПК

3. Описание используемого ПО (перечень использованного лицензионного ПО на рабочем месте, информация о версии операционной системы и наличии критических обновлений, рекомендуемых разработчиком операционной системы)

4. Копия договора на оказание телематических услуг информационно-телекоммуникационной сети Интернет

5. Описание организации доступа в сеть Интернет на рабочем месте

6. Копия чека на оказание доступа в сеть Интернет на повременной основе

7. Копия заявления в правоохранительные органы

8. Копия лицензии на антивирусное ПО

9. Копия чека на антивирусное ПО

10. Описание по антивирусной защите рабочего места (наличие установленного на жестком диске автоматизированного рабочего места клиента антивирусного программного обеспечения и актуальность его баз, частота обновления, сканирования, наличие сведений о проявлении на автоматизированном рабочем месте клиента вредоносных программ)

11. Описание системы защиты информации (наличие или отсутствие персонального межсетевого экрана у клиента, сведения об использовании рабочего места в иных целях, кроме осуществления платежно-расчетных операций, в частности - интернет-серфинга, сведения о порядке хранения и использования ключевых носителей).

**Приложение 5**

**к Условиям предоставления**

**услуг с использованием ДБО**

**Заявление на заключение договора о предоставлении услуг с использованием системы дистанционного банковского обслуживания (ДБО)**

**№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Первоначальное заявление | | | | | Корректирующее | | | | | | | | | |
| ***(Заполняется Клиентом)*** | | | | | |  | | | |  |  | ***(Заполняется банком)*** | | |
| **Наименование Клиента** | | |  | | | | | |  | |  | **№ BSS\_ID** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **ИНН** |  | | | | |  | **КПП** |  | | |  |  | | |
| **КИО** |  | | | | |  |  | | | |  |  | | |
| **Расчетный счет** | |  | | | |  | | | | |  | Операционист | | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Подключить к (наименование Клиента)** | | | | | |  |  | | | |  |  | | |
| **Контактное лицо (Фамилия Имя Отчество)** | | | | | |  |  | | | |  | **№ BSS\_ID** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| **Контактный телефон** | | | |  | |  |  | | | |  |  | | |

Настоящим в соответствии со статьей 428 Гражданского кодекса Российской Федерации Клиент присоединяется к действующей редакции Условий о предоставлении услуг с использованием системы дистанционного банковского обслуживания (ДБО), известных Клиенту и имеющих обязательную для Клиента силу, и просит на указанных условиях заключить с ним договор о предоставлении услуг с использованием системы дистанционного банковского обслуживания (ДБО).

**Клиент подтверждает, что ознакомился с Тарифами Банка и Условиями предоставления услуг с использованием системы дистанционного банковского обслуживания (ДБО)**

Электронная подпись:

**1 подпись:\***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пользователь  Пользователь  Пользователь | (Фамилия И.О.)  (Фамилия И.О.)  (Фамилия И.О.) |  |  | USB-ключ  USB-ключ  USB-ключ |
|  |
|  |

**2 подпись:\***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пользователь  Пользователь  Пользователь | (Фамилия И.О.)  (Фамилия И.О.)  (Фамилия И.О.) |  |  | USB-ключ  USB-ключ  USB-ключ |
|  |
|  |

\* Заполняется в соответствии с карточкой образцов подписей и оттиска печати

|  |  |  |
| --- | --- | --- |
| Дополнительные средства защиты\*\* |  | МАС-адрес (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)  Дополнительный генератор одноразовых паролей eToken PASS  Дополнительный USB – ключ |
|  |
|  |

\*\*Решение о выборе доп. средств защиты клиент принимает самостоятельно.

**Настоящим подтверждаем согласие на предоставление услуг посредством сервиса «Уведомление об операциях по счету» и SMS-авторизации:**

□С одинаковыми правами подписания документов

□ С подписанием документов только персональным ключом электронной подписи

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Телефоны для уведомления об операциях по счету: \*\*\* | **7** |  | **7** |  | **7** |  |
| Телефоны для SMS-авторизации: \*\*\* | **7** |  | **7** |  | **7** |  |
| ФИО владельца телефона для SMS-авторизации |  | |  | |  | |

\*\*\*базовый пакет подключения - услуга предоставляется бесплатно

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Удалить номер телефона: \*\*\*\* | **7** |  | **7** |  | **7** |  |
| Добавить номер телефона: \*\*\* | **7** |  | **7** |  | **7** |  |

\*\*\*\* Минимальное количество телефонов в базовой опции – один. Без подключения базовой опции Договор на оказание услуг с использованием системы ДБО не заключается.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Прошу **подключить** дополнительные опции: | **7** |  | **7** |  | **7** |  |
| Прошу **отключить** дополнительные опции: | **7** |  | **7** |  | **7** |  |

(решение о **подключении/отключении** дополнительных опций Клиент принимает самостоятельно)

|  |  |
| --- | --- |
| **Подсистема «Интернет-Клиент»**   * Изменение пароля пользователя * Учетная запись заблокирована * П/п принято * П/п исполнено * Заявка на покупку/продажу валюты принята * Заявка на покупку/продажу валюты исполнена * Поручение на перевод валюты принято * Поручение на перевод валюты исполнено | **Подсистема «Банк-Клиент»**   * П/п принято * П/п исполнено * Заявка на покупку/продажу валюты принята * Заявка на покупку/продажу валюты исполнена * Поручение на перевод валюты принято * Поручение на перевод валюты исполнено |

Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

М.П.

|  |
| --- |
| ***Заявление принял и проверил* ОТМЕТКИ БАНКА**  **/ /** |
| *(должность работника Банка) (Ф.И.О.) (Подпись) (Дата )* |

**Приложение 6**

**к Условиям предоставления**

**услуг с использованием ДБО**

Пример экранной формы уведомления по счету

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Кредитная организация ПАО "БАЛТИНВЕСТБАНК" Г САНКТ-ПЕТЕРБУРГ  Идентификатор электронного средства платежа :ДБО BS-Client v.3  Идентификатор устройства - \_\_\_\_\_  **Уведомление об операциях по лицевому счету №** | |  | | за период c \_\_\_\_\_ г. по \_\_\_\_\_\_\_\_\_\_ г. включительно. |  | No | ВО | БИК | Банк Контрагента | Контрагент | ИНН контрагента | Счет Контрагента | Дебет | Кредит | Назначение платежа | Тип | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Счет No \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Валюта счета \_\_\_\_\_\_\_\_\_\_ Владелец счета: \_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | | Дата предыдущего движения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2 | | | | | | | | | | | | **Остаток на начало периода \_\_\_\_\_\_\_\_**   | No | ВО | БИК | Банк Контрагента | Контрагент | ИНН контрагента | Счет Контрагента | Дебет | Кредит | Назначение платежа | Тип | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | | | | | | | | | | | | **ИТОГО ОБОРОТЫ *0.00* *0.00*** | | | | | | | | | | | | **Остаток на конец периода \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | | | | | | | | | | | |  | | | | | | | | | | | |  | | | | | | | | | | | |  | | | | | | | | | | | |

Пример печатной формы Уведомления

|  |
| --- |
| Кредитная организация ПАО "БАЛТИНВЕСТБАНК" Г САНКТ-ПЕТЕРБУРГ  Идентификатор электронного средства платежа :ДБО BS-Client v.3  Идентификатор устройства - \_\_\_\_\_  **Уведомление об операциях по лицевому счету №** |
|  |
| за период c \_\_\_\_\_ г. по \_\_\_\_\_\_\_\_\_\_ г. включительно. |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **ВО** | **БИК** | **Банк Контрагента** | **Контрагент** | **ИНН контрагента** | **Счет Контрагента** | **Дебет** | **Кредит** | **Назначение платежа** | **Тип** |

Счет No \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Валюта счета \_\_\_\_\_\_\_\_\_\_\_\_

Владелец счета: \_\_\_\_\_\_\_\_\_\_\_\_\_"

Дата предыдущего движения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Остаток на начало периода \_\_\_\_\_\_\_**

**Дата операций: \_\_\_\_\_\_\_\_\_\_ Данные актуальны на:\_\_\_\_\_\_\_\_\_\_\_**

Остаток на начало дня \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_6

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |

Остаток на конец дня \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ИТОГО ОБОРОТЫ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Остаток на конец периода \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ДОПУСТИМО К СПИСАНИЮ НА \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. 10 минут с момента запроса пароля пользователем [↑](#footnote-ref-1)
2. Тип средства дополнительной защиты, предоставляемый при подключении клиента, остается на усмотрение Банка [↑](#footnote-ref-2)
3. Услуга предоставляется с момента технической доработки Подсистемы «Интернет-клиент». [↑](#footnote-ref-3)