ДОГОВОР №
на обслуживание Клиентов по системе интернет банк ЗАО «КОШЕЛЕВ-БАНК»

г. Самара **«___»_____20__г.**

Закрытое акционерное общество «КОШЕЛЕВ-БАНК», именуемый в дальнейшем **«Банк»**, в лице _____, действующего(ей) на основании _____ с одной стороны, и _____ в лице _____ действующего на основании _____, именуемый в дальнейшем **«Клиент»**, с другой стороны, в дальнейшем именуемые «Стороны», заключили настоящий Договор о нижеследующем.

1. Предмет Договора

1.1. Банк предоставляет Клиенту на платной основе следующие услуги с использованием Системы:

-подключение к системе Интернет–Банк интернет банк ЗАО «КОШЕЛЕВ-БАНК» на основании заявления (*Приложение №3*) настоящего договора;

-прием от Клиента электронных документов, защищенных ЭП, на выполнение операций по счетам Клиента, указанным в *Приложении 3* к настоящему Договору;

-предоставление Клиенту в виде электронных документов, информации об операциях, совершенных по счетам Клиента, указанным в *Приложении 3* к настоящему Договору;

- прием от Клиента и предоставление Клиенту информации свободного формата в виде электронных служебно-информационных документов;

- прием документов и информации, установленных Инструкцией Банка России от 4 июня 2012г. N 138-И «О порядке представления резидентами и нерезидентами уполномоченным банкам документов и информации, связанных с проведением валютных операций, порядке оформления паспортов сделок, а также учета уполномоченными банками валютных операций и контроля за их проведением».

1.2. Электронные документы передаются и принимаются с использованием Системы без их последующего представления на бумажном носителе. Заверенные копии электронных документов на бумажном носителе выдаются Клиенту по письменному запросу по счету(-ам), указанному(-ым) в *Приложении 3* к настоящему Договору, согласно условиям соответствующего Договора банковского счета.

1.3. Настоящий Договор является приложением к Договору(ам) банковского счета, заключенным Сторонами. Во всем ином, что не предусмотрено настоящим Договором, Стороны в своих взаимоотношениях в отношении каждого из указанных в п. 1.1 настоящего Договора Счетов руководствуются положениями, изложенными в Договоре соответствующего банковского счета.

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

2.1. «Система» – система Интернет–Банк «iBank 2», представляющая собой совокупность программно-аппаратных средств, согласованно эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, обеспечивающих создание, передачу и хранение Электронных документов, оформляемых Клиентом и Банком, с целью предоставления Клиенту услуг по Договору банковского счета в соответствии с условиями настоящего Договора.

2.2. «Электронный документ» – документ, в котором информация представлена в электронной форме, содержащий сообщение Банка Клиенту или Клиента Банку, в том числе финансовый документ, информационное или служебное сообщение в Системе, подписанный Электронной подписью, равнозначный документу, подписанному собственноручной подписью.

2.3. «Электронная подпись» (ЭП) – информация, в электронной форме присоединяемая к подписываемому Электронному документу, предназначенная для защиты Электронного документа от подделки, полученная в результате криптографического преобразования информации с использованием Ключа ЭП и позволяющая идентифицировать Владельца Сертификата ключа проверки ЭП, а также установить отсутствие искажения информации в Электронном документе. ЭП, используемая в Системе, отвечает всем требованиям Усиленной неквалифицированной ЭП.

2.4. «ЭП Клиента» – Электронная подпись уполномоченного Клиентом лица (сотрудника Клиента).

2.5. «Владелец сертификата ключа проверки ЭП» – физическое лицо, владеющее соответствующим Ключом ЭП, позволяющим создавать свою ЭП в Электронных документах (подписывать Электронные документы), на имя которого Банком и Клиентом составлен Сертификат ключа проверки ЭП сотрудника Клиента.

2.6. «Владелец сертификата ключа проверки ЭП без права подписи» – физическое лицо, владеющее соответствующим Ключом ЭП, предоставляющим право работы с Электронными документам Клиента, за исключением права подписывать Электронные документы.

2.7. «Ключ ЭП Клиента» – ключ, генерируемый Клиентом (сотрудником Клиента) с использованием средств Системы, представляющий собой уникальную последовательность символов, предназначенную для создания ЭП в Электронном документе.

2.8. «Ключ проверки ЭП Клиента» – ключ, генерируемый Клиентом (сотрудником Клиента) с использованием средств Системы, представляющий собой уникальную последовательность символов, однозначно связанную с Ключом ЭП Клиента, и предназначенную для подтверждения подлинности ЭП в Электронном документе.

2.9. «Сертификат ключа проверки ЭП сотрудника Клиента» (далее - Сертификат) – документ на бумажном носителе, подписанный Владельцем Ключа ЭП Клиента и заверенный подписью руководителя и оттиском печати Клиента, с указанным в шестнадцатеричном виде Ключом проверки ЭП Клиента, подтверждающий принадлежность Ключа проверки ЭП Владельцу сертификата ключа проверки ЭП; (форма Сертификата ключа – *Приложение 4*).

2.10. «Пара ключей ЭП Клиента» – Ключ ЭП Клиента и соответствующий ему Ключ проверки ЭП Клиента.

2.11. «Корректная ЭП Клиента» – ЭП электронного документа Клиента, проверка которой, с использованием соответствующего Ключа проверки ЭП Клиента, дает положительный результат.

2.12. «Активный Ключ проверки ЭП Клиента» – Ключ проверки ЭП Клиента, зарегистрированный Банком в Системе и используемый Клиентом в текущее время для работы в Системе.

2.13. «Группа подписи» – полномочия ЭП уполномоченного лица Клиента, определяемые организационно-распорядительными документами Клиента:

- группа подписи № 1 – уполномоченное/ые лицо/а Клиента, обладающее/ие правом первой подписи;
- группа подписи № 2 – уполномоченное/ые лицо/а Клиента, обладающее/ие правом второй подписи;
- группа без права подписи – уполномоченное/ые лицо/а Клиента, обладающее/ие правом работы с Электронными документами Клиента, за исключением права подписывать Электронные документы.

В случае, когда организационно-распорядительными документами Клиента предусмотрено наличие на Электронных документах двух ЭП, их полномочия определяются группой подписи: для формирования первой ЭП используется Ключ ЭП Клиента из группы подписи № 1, для формирования второй ЭП используется Ключ ЭП Клиента из группы подписи № 2.

2.14. «Блокировочное слово» – уникальное слово, определяемое Клиентом при регистрации в Системе, для блокирования работы Клиента по телефонному звонку в Банк.

2.15. Компрометация ключа ЭП – утрата, хищение, несанкционированное копирование, передача ключа ЭП по каналам связи в открытом виде, любые другие виды разглашения содержания Ключа ЭП, а также утрата или повреждение носителей, содержащих ключевую информацию.

2.16. USB-токен – аппаратное USB-устройство генерации и хранения ключей ЭП, использование которого при условии соблюдения требований правил эксплуатации и хранения USB-токена «iBank2 Key» обеспечивает защищенное хранение и неизвлекаемость Ключа ЭП Клиента.

2.17. «Тарифы» – размеры комиссионных вознаграждений за банковское обслуживание по Системе, установленные Банком, а также другие условия, оговоренные в Тарифах и условиях на банковские услуги.

3. Согласия Сторон

3.1. Стороны признают, что используемые в Системе средства криптографической защиты информации (СКЗИ), которые обеспечивают шифрование, контроль целостности и Электронную подпись, достаточны для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства Электронных документов, а также разбора конфликтных ситуаций.

3.2. Стороны признают, что при произвольном изменении Электронного документа, заверенного Электронной подписью, ЭП становится некорректной, то есть проверка ЭП дает отрицательный результат.

3.3. Стороны признают, что подделка ЭП Клиента, то есть создание Корректной ЭП Электронного документа от имени Клиента, практически невозможно без знания Ключа ЭП Клиента.

3.4. Стороны признают, что Электронные документы, заверенные необходимым количеством Электронных подписей Клиента, юридически эквивалентны соответствующим документам на бумажном носителе, подписанным Клиентом и имеющим оттиск печати Клиента, обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества Электронных подписей Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

3.5. Стороны признают, что Электронные документы с Электронными подписями Клиента, создаваемые Системой и хранящиеся в Банке, являются доказательным материалом для решения спорных вопросов в соответствии с *Приложением 2* – «Положение о порядке проведения технической экспертизы при возникновении спорных ситуаций» – к настоящему Договору. Электронные документы, не имеющие необходимого количества Электронных подписей, при наличии спорных вопросов не являются доказательным материалом.

3.6. Стороны признают, что Ключ проверки ЭП Клиента, указанный в заверенном подписью руководителя и оттиском печати Клиента Сертификате ключа проверки ЭП сотрудника Клиента, принадлежит Клиенту.

3.7. Стороны признают, что Перечень видов Электронных документов, передаваемых по Системе, определяется возможностями Системы и может изменяться Банком с предварительным уведомлением Клиента сообщением по Системе.

3.8. Стороны признают в качестве единой шкалы времени при работе с Системой Самарское поясное время. Контрольным является время системных часов аппаратных средств Банка.

3.9. Стороны признают, что использование всемирной телекоммуникационной сети общего доступа Интернет может вызывать перерывы в приеме и обработке Электронных документов в Системе, связанные с отказами телекоммуникационного оборудования провайдеров телекоммуникационных услуг, а также вирусными и иными атаками на Систему. Стороны обязаны принимать все доступные способы защиты от указанных угроз.

3.10. Стороны признают, что на дату заключения настоящего Договора Банком установлено следующее операционное время:

- для электронных платежных документов в валюте Российской Федерации, Евро и долларах США: с 9 ч. 00 мин. до 16 ч. 00 мин., если иное не установлено внутренним распоряжением Банка.

4. Права и обязанности Банка:

4.1. Банк обязан исполнять принятые от Клиента Электронные документы, подписанные Корректной ЭП Клиента, в соответствии с условиями настоящего Договора, Договоров банковского счета и действующим законодательством.

4.2. Банк обязан по получении от Клиента Уведомления по форме *Приложения 5* (допускается передача Уведомления по факсу), либо по поступлению телефонного звонка с указанием Блокировочного слова и при условии соблюдения требований п. 5.3. настоящего Договора, блокировать Активный Ключ проверки ЭП Клиента в Системе. Банк не обязан проверять подлинность подписи Клиента на полученном по факсу Уведомлении, а обязан только установить путем обычного визуального контроля соответствие подписи имеющемуся у Банка образцу. Блокирование Ключа проверки ЭП Клиента не влечет недействительности Электронных документов, содержащих Корректную ЭП Клиента, переданных по Системе до момента блокирования Ключа проверки ЭП Клиента. Наложенная блокировка снимается только на основании письменного заявления Клиента не позднее дня, следующего за днем получения такого требования. Временная блокировка ключа ЭП не отменяет Тарифа за пользование Системой на период блокирования.

4.3. Банк обязан обеспечить строго контролируемый и ограниченный доступ к помещениям, в которых находятся программно-аппаратные средства, содержащие контрольные архивы Системы.

4.4. Банк обязан хранить в секрете и не передавать третьим лицам Ключ проверки ЭП Клиента, используемый при работе в Системе.

4.5. Банк обязан предоставить Клиенту СКЗИ и руководство (инструкцию) по эксплуатации Системы (вид носителя определяется Банком самостоятельно), а также рекомендации и консультации, необходимые для работы с Системой (телефон для консультаций: (846) 956-78-88, электронный адрес: dbo@koshelev-bank.ru). Консультации оказываются в рабочие часы Банка.

4.6. Банк обязан ознакомить Клиента с Требованиями Банка об идентификации лиц, имеющих право работать в Системе, используя электронную подпись (*Приложение 1*).

4.7. Банк вправе не принимать Сертификат ключа проверки ЭП сотрудника Клиента, если образцы подписи Владельца сертификата ключа проверки ЭП или руководителя Клиента вызывают сомнения у уполномоченного сотрудника Банка.

4.8. Банк имеет право отказать в исполнении Электронного документа Клиента в случае несоответствия реквизитов такого документа обязательным реквизитам, установленным действующим законодательством РФ и банковскими правилами.

4.9. Банк вправе без уведомления Клиента блокировать Активный Ключ проверки ЭП Клиента при наличии достаточных оснований считать, что посредством Системы состоялась или возможна попытка несанкционированного доступа к Счетам Клиента, и потребовать от Клиента замены Пары ключей ЭП.

4.10. Банк вправе в одностороннем порядке расторгнуть настоящий Договор, прекратить действие Ключей ЭП и банковское обслуживание Клиента по Системе, направив уведомление в письменной форме, в случаях:

- неисполнения Клиентом обязанностей, установленных настоящим Договором, и/или Договором банковского счета;
- возникновения у Банка подозрений, что деятельность Клиента может быть связана с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

4.11. Банк имеет право расторгнуть Договор в одностороннем порядке и прекратить обслуживание Клиента по Системе без предварительного уведомления Клиента в случае невнесения платы за пользование Системой. При этом Клиенту направляется письменное уведомление о расторжении Договора.

4.12. Банк вправе отказать Клиенту в заключении Договора или расторгнуть действующий Договор в одностороннем порядке при невыполнении Клиентом положений настоящего Договора.

4.13. Банк вправе в одностороннем порядке вводить новые, изменять и дополнять действующие Тарифы на услуги Банка, порядок и сроки взимания платы, уведомив об этом Клиента не позднее 10 дней до даты вступления в силу соответствующих изменений. Уведомление об установлении Тарифов по настоящему Договору направляется Банком Клиенту в виде электронного служебно-информационного документа с использованием Системы.

5. Права и обязанности Клиента

5.1. Клиент имеет право требовать от Банка предоставления на бумажном носителе копий Электронных документов, согласно выбранным в Заявлении (*Приложение 3*) условиям с проставлением на них соответствующих отметок Банка (об исполнении и др.). Указанные документы предоставляются уполномоченному лицу Клиента при его явке в Банк.

5.2. Клиент имеет право досрочно прекращать действие Ключа проверки ЭП Клиента (вместе с соответствующим Ключом ЭП Клиента), направив Уведомление по форме *Приложения 5*. Для продолжения работы Клиента в Системе уполномоченный представитель Клиента должен сгенерировать новую Пару ключей ЭП Клиента и передать Банку новый Сертификат ключа проверки ЭП сотрудника Клиента.

5.3. В исключительных случаях (утрата или компрометация Ключей ЭП) Клиент имеет право блокировать Ключ проверки ЭП Клиента, т.е. приостановить работу в Системе, направив письменное Уведомление по форме *Приложения 5* или позвонив по телефону с произнесением Блокировочного слова в офис Банка, осуществляющий обслуживание Клиента. Номера телефона сообщаются Клиенту при подписании настоящего Договора. Клиент обязан зафиксировать время, ФИО и должность сотрудника Банка, принявшего телефонный звонок. Блокировка снимается не позднее дня, следующего за днем получения Банком письменного требования Клиента о снятии блокировки.

5.4. Клиент обязан при создании Электронных документов в Системе соблюдать условия настоящего Договора, нормы действующего законодательства и банковские правила в отношении обязательных реквизитов данных документов. Соблюдать Требования по обеспечению безопасности в процессе эксплуатации Системы.

5.5. Клиент обязан организовывать внутренний режим функционирования рабочих мест уполномоченных лиц таким образом, чтобы исключить возможность использования Системы и ключей ЭЦП лицами, не имеющими допуска к работе с ними. Риск неблагоприятных последствий, связанных с использованием Ключа ЭП Клиента неуполномоченными лицами, несет Клиент (Памятка Клиенту о возможных угрозах и способах защиты – Приложение 6).

5.6. Клиент обязан сообщать Банку об обнаружении попытки несанкционированного доступа к Системе или к Ключу ЭП Клиента в день ее обнаружения и блокировать свою работу в Системе, направив в Банк Уведомление по форме *Приложения 5*, либо позвонив по телефону с произнесением Блокировочного слова. Клиент несет риск всех последствий, связанных с несанкционированным доступом к Системе или Ключу ЭП Клиента.

5.7. Клиент обязан по требованию Банка приостановить работу в Системе и для ее возобновления сгенерировать новую Пару ключей ЭП Клиента и передать Банку новый Сертификат ключа проверки ЭП сотрудника Клиента.

5.8. Клиент обязан сгенерировать новую Пару ключей ЭП Клиента и передать Банку новый Сертификат ключа проверки ЭП сотрудника Клиента при наступлении Даты окончания действия ранее представленного Сертификата.

5.9. Клиент обязан уведомлять Банк о смене лиц, уполномоченных работать с Системой и распоряжаться Счетом, и для возможности работы с Системой новых лиц предоставить им возможность сгенерировать Пару ключей ЭП Клиента.

5.10. Клиент обязан в случае расторжения договора или прекращения использования Системы уничтожить программное обеспечение Системы, включая СКЗИ.

5.11. Клиент обязан регулярно производить оплату за пользование Системой в соответствии с утвержденными Банком Тарифами.

5.12. Клиент обязан обеспечить изучение лицами, уполномоченными работать с Системой, руководства (инструкции) по использованию Системы, предоставленного Банком, а также соблюдение требований безопасности и рекомендаций Банка по работе в Системе.

5.13. Клиент обязан до подписания настоящего Договора ознакомиться с Требованиями Банка об идентификации лиц, имеющих право работать в Системе, используя электронную подпись (*Приложение 1*), строго соблюдать и обеспечить своевременное и надлежащее выполнение вышеуказанных Требований при работе в Системе.

6. Совместные обязательства и ответственность Сторон

6.1. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои аппаратные и программно-технические средства, используемые при работе с Системой.

6.2. В случае возникновения конфликтных ситуаций между Сторонами при использовании Системы Стороны обязуются участвовать в рассмотрении конфликтов в соответствии с «Положением о порядке проведения технической экспертизы при возникновении спорных ситуаций» (*Приложение 2*), выполнять требования указанного Положения и нести ответственность согласно выводам по рассмотрению конфликтной ситуации. В случае, если Клиент отказывается от принятия на себя обязательств по Электронному документу (оспаривает факт или время передачи Электронного документа, его содержание), бремя доказывания обстоятельств, на основании которых он отказывается от принятия на себя обязательств, ложится на него. Ответственность может быть возложена на Банк в случае, если создание Электронного документа обусловлено его противоправными действиями.

6.3. Стороны обязуются при разрешении споров, которые могут возникнуть в связи с использованием Системы, предоставлять в письменном виде свои оценки, доказательства и выводы по запросу противоположной Стороны.

6.4. Банк не несет ответственности за ущерб, возникший вследствие компрометации ключа ЭП клиента, использования его, утраты или передачи неуполномоченным лицам, вне зависимости от причин, также Банк не несет ответственности за последствия исполнения электронного платежного документа, подписанного корректной ЭП Клиента, в т.ч. в случае использования ключей ЭП неуполномоченным лицом.

БАНК _____ _____ КЛИЕНТ _____

6.5. Банк не несет ответственности за неработоспособность оборудования и программных средств Клиента и третьих лиц, повлекшую за собой невозможность доступа Клиента к банковской части Системы и возникшие в результате задержки в осуществлении платежей Клиента, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Клиента, подключенных к сети Интернет для обеспечения предоставления услуг по настоящему Договору.

6.6. Банк не несет ответственности в случае реализации угроз несанкционированного доступа неуполномоченных лиц к части Системы, установленной у Клиента, и ключам ЭП Клиента, включая угрозы со стороны внутренних (локальных) и внешних (глобальных) сетей связи.

6.7. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору при наступлении и в период влияния последствий обстоятельств непреодолимой силы, таких как стихийные бедствия, пожар, военные действия, массовые беспорядки, народные волнения, принятие органами государственной власти и управления нормативных актов, препятствующих исполнению обязательств по настоящему Договору, других обстоятельств, общепризнанных кризисными. Сторона, пострадавшая от влияния обстоятельств непреодолимой силы, обязана в возможно короткий срок, но не более чем через 7 (Семь) дней после возникновения этих обстоятельств, довести до сведения другой Стороны информацию о случившемся.

7. Порядок обслуживания Клиента

7.1. Для начала работы по настоящему Договору Клиент обязан произвести оплату за подключение к Системе в соответствии с Тарифами Банка и предоставить Банку Сертификат(ы) ключа проверки ЭП сотрудника Клиента в порядке, предусмотренном *Приложением 1* к Договору. До этого момента Банк не принимает Электронные документы Клиента. Сертификат ключа проверки ЭП сотрудника Клиента действителен для предъявления в Банк в течение одного месяца с момента его формирования. Поле «Дата начала действия» Сертификата ключа проверки ЭП сотрудника Клиента заполняется уполномоченным лицом Банка. Дата начала действия равна дате представления Сертификата в Банк. Поле «Дата окончания действия» Сертификата ключа проверки ЭП заполняется уполномоченным лицом Банка. Дата может принимать только одно из следующих значений:

- Дата начала действия Сертификата плюс 1 год;

или

- Дата окончания срока действия полномочий лица – Владельца сертификата ключа проверки ЭП. Указанная дата определяется на основании учредительных, организационно-распорядительных (приказов, протоколов заседаний органов управления, доверенностей) и иных документов, находящихся в юридическом деле Клиента по открытому Счету, если указанная дата наступает ранее истечения 1 года с Даты начала действия Сертификата.

7.2. Банк активирует Ключи проверки ЭП Клиента не позднее следующего рабочего дня после их приема при условии исполнения Клиентом *Приложения 1*. Оплата за пользование Системой производится со дня активации Ключей.

7.3. При получении Банком документов, подтверждающих прекращение полномочий какого-либо из представителей Клиента – Владельца сертификата ключа проверки ЭП, Банк прекращает прием Электронных документов, подписанных ЭП данного лица. При предоставлении Клиентом полномочий по работе с Системой новому лицу с правом первой или второй подписи Электронных документов, Банк начинает прием от Клиента Электронных документов, подписанных ЭП данного лица, не позднее рабочего дня, следующего за днем получения Банком соответствующих документов, подтверждающих указанное право данного лица и Сертификата ключа проверки ЭП сотрудника Клиента, оформленного в порядке, предусмотренном *Приложением 1* к Договору. При предоставлении Клиентом полномочий по работе с Системой новому лицу без права подписи Электронных документов, Банк предоставляет возможность работы с Системой данному лицу не позднее рабочего дня, следующего за днем получения Банком соответствующих документов, подтверждающих указанное право, и Сертификата ключа проверки ЭП сотрудника Клиента. Банк прекращает прием Электронных документов, подписанных ЭП уполномоченного лица Клиента, при наступлении Даты окончания действия соответствующего Сертификата ключа проверки ЭП сотрудника Клиента.

7.4. Банк осуществляет прием Электронных документов, передаваемых по Системе, круглосуточно. Использование Системы не лишает Клиента права предоставлять Банку расчетные и иные документы на бумажном носителе. Исполнение документов осуществляется в сроки, установленные Договором банковского счета.

7.5. При получении Электронного документа Банк производит проверку:

- корректности ЭП Клиента Ключом проверки ЭП Клиента;
- правильности заполнения реквизитов Электронного документа;
- иные проверки, предусмотренные Договором банковского счета.

7.6. Банк средствами Системы (статус документа, электронное письмо и др.) информирует Клиента об исполнении/неисполнении переданного им по Системе Электронного документа. Иного информирования Клиента о неисполнении Электронного документа Банком не осуществляется. Клиент обязан самостоятельно отслеживать смену статусов документов в Системе и осуществлять контроль принятия Банком документов к исполнению.

7.7. Дальнейшее оформление Электронных документов, переданных в Банк по Системе, осуществляется Банком без участия Клиента, в том числе оформление копий таких документов на бумажном носителе для передачи иным участникам расчетов.

7.8. Если по истечении 3 (Трех) рабочих дней с момента проведения Банком операции (отказа в проведении операции) по Счету на основании полученного от Клиента Электронного документа, Клиент не заявляет претензий по такой операции, признается, что Клиент подтвердил правомерность действий Банка и(или)

правильность проведения операции по его Счету. По истечении указанного срока претензии от Клиента Банком не принимаются и не рассматриваются по существу.

7.9. Клиент имеет право с использованием Системы самостоятельно получать информацию о состоянии своего Счета в течение текущего операционного дня. Периодичность обновления информации в Системе устанавливается Банком. Полученная в результате запроса Клиента выписка за текущий операционный день носит предварительный характер и не порождает ответственности со стороны Банка.

7.10. Датой получения Клиентом от Банка документов, установленных Инструкцией Банка России от 4 июня 2012г. N138-И «О порядке представления резидентами и нерезидентами уполномоченным банкам документов и информации, связанных с проведением валютных операций, порядке оформления паспортов сделок, а также учета уполномоченными банками валютных операций и контроля за их проведением», является дата изменения статуса документа.

8. Действие Договора

8.1. Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и заключается на неопределенный срок.

8.2. Каждая из Сторон вправе расторгнуть настоящий Договор в одностороннем порядке не ранее, чем через 5 (Пять) рабочих дней после письменного уведомления об этом противоположной Стороны (за исключением случая, описанного в п. 4.11). При этом обязательства по настоящему Договору, возникшие в период его действия, не прекращаются до полного исполнения их Сторонами.

8.3. Расторжение настоящего Договора не влечет недействительности Электронных документов, содержащих Корректную ЭП Клиента, переданных Клиентом по Системе до дня расторжения настоящего Договора включительно.

8.4. Настоящий Договор прекращает свое действие в случае расторжения всех указанных в п. 1.1 Договоров банковского счета. Отказ Клиента от обслуживания по Системе не влечет прекращения расчетно-кассового обслуживания.

9. Заключительные положения

9.1. Споры по настоящему Договору решаются путем переговоров. Претензии Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки ЭП Клиента под Электронным документом, рассматриваются в порядке, установленном *Приложением 4*. При недостижении согласия Сторон по спору в течение 1 (Одного) месяца с момента получения Стороной претензии в письменной форме спор передается на рассмотрение в Арбитражный суд Самарской области. Стороны признают, что положения, установленные настоящим пунктом, фактически являются для Сторон соглашением об обязательном соблюдении досудебного порядка рассмотрения возможных споров, вытекающих из настоящего Договора, и об их подсудности.

9.2. Все приложения, изменения и дополнения к настоящему Договору оформляются в письменном виде, подписываются полномочными представителями сторон и являются его неотъемлемой частью.

9.3. Настоящий Договор составлен в двух экземплярах по одному для каждой Стороны, оба экземпляра имеют одинаковую юридическую силу.

10. Адреса и реквизиты Сторон

Банк: **ЗАО «КОШЕЛЕВ-БАНК»** **Местонахождение:443035,г.Самара, ул. Мирная, д.162** **Почтовый адрес: 443035, г.Самара, ул. Мирная, д.162** **Реквизиты:** **ИНН 5260059340 /КПП 631201001** **БИК 043601742** **К/с 30101810236010000742** **в Отделении по Самарской области Волго-Вятского главного управления Центрального банка Российской Федерации (Отделение Самара)**	**Клиент:** **Юридический:**_____ _____ **Почтовый:** _____ _____ **Реквизиты:** **ИНН _____ / КПП _____** **р/с № _____** **в ЗАО «КОШЕЛЕВ-БАНК» БИК 043601742** **Тел. _____**

от Банка:

_____/_____/

М.П.

от Клиента:

_____/_____ /

М.П.

БАНК _____ _____ КЛИЕНТ _____

Приложение № 1
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от «___»_____**20___г.**

ТРЕБОВАНИЯ ОБ ИДЕНТИФИКАЦИИ ЛИЦ, ИМЕЮЩИХ ПРАВО РАБОТАТЬ В СИСТЕМЕ, ИСПОЛЬЗУЯ ЭЛЕТРОННУЮ ПОДПИСЬ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Требования разработаны в соответствии с положениями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Положением Банка России от 19.08.2004 № 262-П «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Инструкции Банка России от 30.05.2014 № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам)».

1.2. Настоящие Требования применяются к отношениям сторон (Банка и Клиента), возникшим при заключении и/или исполнении Договора на обслуживание Клиентов в системе интернет банк ЗАО «КОШЕЛЕВ-БАНК» (далее – Договор).

2. ПРАВООТНОШЕНИЯ (ВЗАИМОДЕЙСТВИЯ) СТОРОН

2.1. Клиент обязан обеспечить подписание Договора, любых Дополнительных соглашений к нему, а также Заявления на подключение к Системе Единоличным исполнительным органом Клиента – организации, индивидуальным предпринимателем или лицом, уполномоченным на подписание Договора (Дополнительного соглашения к нему) только в присутствии представителя Банка.

2.2. Клиент обязан предоставить документ, удостоверяющий личность Единоличного исполнительного органа юридического лица или индивидуального предпринимателя, а также уполномоченных им лиц на право работать в Системе, с которого уполномоченным представителем Банка снимается копия в присутствии указанных лиц.

2.3. Клиент обязан предоставить в Банк документы (надлежащим образом заверенные копии документов), подтверждающие полномочия указанных лиц для работы в Системе. Сертификат ключа проверки ЭП сотрудника Клиента в Системе интернет банк ЗАО «КОШЕЛЕВ-БАНК» подписывается лицом, имеющим право работать в Системе, и Единоличным исполнительным органом Клиента – юридического лица или индивидуальным предпринимателем в присутствии представителя Банка.

2.4. В случае, если Клиент блокировал Ключ проверки ЭП Клиента в соответствии с пунктом 5.3 Договора, письменное заявление Клиента о снятии блокировки подписывается Единоличным исполнительным органом Клиента – юридического лица или индивидуальным предпринимателем в присутствии представителя Банка. Заявление Клиента о снятии блокировки может быть подписано также в присутствии представителя Банка лицом, уполномоченным распоряжаться денежными средствами, находящимися на Счете Клиента с использованием ЭП Клиента при условии, что такое право ему предоставлено соответствующей доверенностью и указанное лицо ранее было идентифицировано Банком в соответствии с пунктом 2.3. настоящих Требований (Сертификат ключа проверки ЭП сотрудника Клиента в Системе интернет банк ЗАО «КОШЕЛЕВ-БАНК» был ранее подписан указанным лицом в присутствии представителя Банка и Единоличного исполнительного органа Клиента – юридического лица или индивидуального предпринимателя, и такой Сертификат является действительным на момент подачи заявления о снятии блокировки).

2.5. Настоящие Требования применяется также при оформлении нового Сертификата ключа проверки ЭП сотрудника Клиента в случае окончания срока его действия, в том числе в случае его компрометации (отмены) в соответствии с положениями Договора.

2.6. Настоящие требования применяются также в случае, если в качестве Единоличного исполнительного органа Клиента выступает управляющая организация или управляющий.

2.7. Несоблюдение Клиентом настоящих Требований является основанием для отказа Клиенту в заключении Договора, а также для расторжения Банком действующего Договора в одностороннем порядке.

С настоящими Требованиями ознакомлен

Директор _____/_____/
подпись представителя Клиента

БАНК _____ _____ КЛИЕНТ _____

Приложение № 2
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от «___»_____20___г.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ ВОЗНИКНОВЕНИИ СПОРНЫХ СИТУАЦИЙ

1. В настоящем Положении под спорной ситуацией понимается существование претензий у Клиента к Банку (вместе в дальнейшем именуются Сторонами), справедливость которых может быть однозначно установлена в результате проверки Электронных цифровых подписей Клиента в Электронных документах.

2. Клиент представляет Банку в письменном виде заявление, содержащее существо претензии с указанием на Электронный документ, на основании которого Банк выполнил операции по счёту Клиента. В заявлении также должно быть указано лицо (лица), уполномоченное представлять интересы Клиента в разрешительной комиссии.

3. Банк обязан в течение пяти рабочих дней с момента получения заявления Клиента сформировать разрешительную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка. По специальному требованию одной из Сторон с состав комиссии могут быть включены независимые эксперты. Независимый эксперт должен иметь высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет.

4. Банк обязан письменно, не позднее, чем за три рабочих дня до начала работы разрешительной комиссии, уведомить Клиента о назначенной дате, времени и месте начала работы комиссии.

5. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов.

6. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в Системе интернет банк ЗАО «КОШЕЛЕВ-БАНК».

7. В случае если Клиент не направит своих представителей для участия в работе разрешительной комиссии, рассмотрение спорной ситуации осуществляется без представителей Клиента. В этом случае в Акте делается запись об отсутствии представителя Клиента.

8. В результате рассмотрения спорной ситуации разрешительная комиссия должна определить подлинность ЭЦП Клиента под приложенным Электронным документом и правомерность выполнения Банком операций по счету Клиента.

9. Разрешительная комиссия проводит рассмотрение заявления в срок не более пяти рабочих дней с момента формирования комиссии. Рассмотрение заявления включает следующие этапы:

9.1. Разрешительная комиссия проводит техническую экспертизу ключа (ключей) ЭЦП Клиента.

9.1.1. С использованием штатного программного обеспечения Системы «iBank 2» АРМ «Регистратор» выполняется распечатка Сертификата Открытого ключа ЭЦП Клиента, соответствующего Закрытому ключу ЭЦП клиента, которым был подписан спорный Электронный документ. По согласованию Сторон печатная форма Сертификата может быть получена с использованием ПО АРМ «Администратор».

9.1.2. Распечатанный сертификат сверяется с Сертификатом Открытого ключа ЭЦП Клиента, заверенным подписью уполномоченного лица Клиента и являющимся приложением к договору. Сверяются ID ключа и его шестнадцатеричное представление. При обнаружении расхождений ситуация далее не рассматривается, комиссия составляет акт о выявленном несоответствии.

9.2. Разрешительная комиссия проводит техническую экспертизу Электронного документа, заверенного необходимым количеством соответствующих Электронных цифровых подписей Клиента, на основании которого Банком выполнены операции по счету Клиента.

9.2.1. С использованием штатного ПО Системы интернет банк ЗАО «КОШЕЛЕВ-БАНК» АРМ «Операционист» выбирается спорный документ и выполняется операция «Проверить ЭЦП».

По требованию одной из Сторон, комиссией могут использоваться специализированные эталонные утилиты от разработчика Системы «iBank 2» для выгрузки документа из Базы данных Системы интернет банк ЗАО «КОШЕЛЕВ-БАНК» и автономной проверки в соответствии с сопроводительной документацией.

9.2.3. По взаимному согласию членов комиссии, автономную проверку подлинности ЭЦП может провести независимая организация, в том числе разработчик системы «iBank 2» - ООО «БИФИТ». Эксперт, проводящий автономную проверку подлинности ЭЦП, должен иметь высшее профессиональное образование или профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области не менее 5 лет.

В этом случае Банком не позднее пяти рабочих дней с момента принятия согласованного решения о проведении независимой экспертизы в независимую организацию направляются материалы для проведения проверки, полученные в результате выгрузки спорного документа из базы данных системы интернет банк «ЗАО «КОШЕЛЕВ-БАНК», копии Сертификатов Открытого ключа ЭЦП Клиента, заверенные обеими Сторонами, и подписанное обеими Сторонами письмо с просьбой о проведении проверки. По результатам проверки независимая организация формирует заключение о подлинности ЭЦП в предоставленном документе и высылает его в адрес Банка.

Срок проведения независимой экспертизы не должен превышать одного календарного месяца с момента принятия согласованного решения о проведении независимой экспертизы.

БАНК _____ _____ КЛИЕНТ _____

9.3. На основании данных технической экспертизы разрешительная комиссия составляет акт, содержащий

– фактические обстоятельства, послужившие основанием возникновения разногласий;

– все реквизиты оспариваемого документа;

– порядок работы членов комиссии;

– вывод о подлинности ЭЦП в оспариваемом Электронном документе и его обоснование.

В случае если проводилась независимая проверка подлинности ЭЦП, к Акту прилагается подготовленное независимой организацией заключение о подлинности ЭЦП

Акт составляется непосредственно после завершения оценки всех обстоятельств, подлежащих установлению согласительной комиссией, в двух экземплярах по экземпляру для каждой Стороны и подписывается всеми членами комиссии.

10. Банк несет ответственность перед Клиентом в случае, когда имела место хотя бы одна из следующих ситуаций:

10.1. Банк не предъявляет Электронный документ, подписанный Клиентом, на основании которого Банк выполнил операции по счёту Клиента.

10.2. Банк не предъявляет Сертификаты Открытого ключа ЭЦП Клиента, заверенные подписью руководителя и имеющие оттиск печати Клиента, соответствующие Секретным ключам ЭЦП Клиента, которыми был подписан спорный Электронный документ.

10.3. Хотя бы одна ЭЦП Клиента в Электронном документе оказалась не подлинной.

10.4. Клиент предоставляет Уведомление об отмене действия Секретного и соответствующего ему Открытого ключа ЭЦП Клиента, подписанное уполномоченным должностным лицом Банка и имеющее оттиск печати Банка. При этом указанная в Уведомлении дата окончания действия Пары ключей ЭЦП Клиента раньше даты подписи, указанной в рассматриваемом Электронном документе.

11. В случае, когда Банк предъявляет Электронный документ и Сертификаты Открытого ключа ЭЦП Клиента, подлинность ЭЦП Клиента в Электронном документе признана разрешительной комиссией, принадлежность Клиенту Открытых ключей ЭЦП Клиента подтверждена, Банк не несёт ответственности перед Клиентом по выполненным операциям по счёту Клиента.

12. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими ЭЦП о компрометации Секретного ключа (ключей) ЭЦП Клиента, что не снимает с Клиента ответственности за данный документ.

БАНК _____ _____ КЛИЕНТ _____

Приложение № 3
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от «___»_____20___г.

ЗАЯВЛЕНИЕ №_____

_____
(наименование Клиента)

на основании Договора на обслуживание Клиентов в системе интернет банк ЗАО «КОШЕЛЕВ-БАНК», прошу:

- [V] - подключить к Системе следующие счета:
- [ ] - внести изменения в ранее предоставленное заявление:
- [ ] - отключить от Системы следующие счета:

Расчетный №																			

- [V] - предоставить право работы в Системе указанным лицам:
- [ ] - прекратить право работы в Системе указанных лиц:
- [ ] - внести изменения в сведения и состав лиц, имеющих право работы в Системе:

Сведения о владельцах сертификата ключа ЭП – с правом подписи:

ФИО _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____	**ФИО** _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____

Сведения о владельцах сертификата ключа ЭП – с правом подписи:

ФИО _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____	**ФИО** _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____

Сведения о владельцах сертификата ключа ЭП – без права подписи:

ФИО _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____	**ФИО** _____ **Документ, удостоверяющий личность** _____ **серия**_____ **№** _____, **выдан**_____ _____, **дата выдачи** _____._____._____

Телефон контакта ответственного сотрудника Клиента:

Тел № _____

БАНК _____ _____ КЛИЕНТ _____

☑ - прошу выдать средства защиты от несанкционированного доступа USB- токены, в количестве: _____ штук
(в случае присоединения к другому Клиенту для использования USB-токена – указывается 0 штук)

Получил средства защиты от несанкционированного доступа USB- токены:

Директор _____/_____/
подпись представителя Клиента

ПЕРЕЧЕНЬ Клиентов, для которых допускается совместное использование USB-токенов по Договорам о предоставлении услуг с использованием Системы.

Наименование Клиента, заключившего договор	**Номер и дата договора**

☐ - прошу подключить услугу подтверждения аутентификации SMS-паролем на вход в Систему:

☐ - прошу отключить услугу подтверждения аутентификации SMS-паролем на вход в Систему:

☐ - прошу подключить услугу подтверждения платежного документа одноразовым SMS-паролем:

☐ - отключить услугу подтверждения платежного документа одноразовым SMS-паролем:

Телефон 1 № _____ группа подписи 1	**Телефон 2 № _____ группа подписи 2**
Телефон 3 № _____ группа подписи 1	**Телефон 4 № _____ группа подписи 2**

☐ -прошу подключить дополнительную услугу IP-фильтрации со следующими IP-адресами:

☐ - прошу отключить дополнительную услугу IP-фильтрации со следующими IP-адресами:

IP 1:	**IP 2:**	**IP 3:**
IP 4:	**IP 5:**	**IP 6:**

(При попытке входа в Систему «iBank2» с использованием иных IP-адресов, считать операцию надлежащим образом не подтвержденной, и Проведение операций по счетам с использованием Системы интернет банк ЗАО «КОШЕЛЕВ-БАНК» не осуществлять.)

☐ -прошу подключить Систему интернет-банка ЗАО «КОШЕЛЕВ-БАНК» силами специалистов банка:
(дополнительно взимается комиссия за установку согласно тарифов банка)

Директор _____/_____/
подпись представителя Клиента

Дата _____._____

М.П.

Заявление принял и проверил:
ОТМЕТКИ БАНКА

_____ _____ /_____/_____
(должность работника Банка) **(ФИО)** **(Подпись)** **(Дата)**

БАНК _____ _____ КЛИЕНТ _____

Приложение № 4
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от «___»_____20___г.

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ "iBank 2"

1.Наименование организации_____
2. Место нахождения юр. лица_____
3.ОГРН_____ дата внесения в ЕГРЮЛ (ЕГРИП) "___"_____года
4.Тел._____ 5. ИНН (КИО)_____6. КПП*_____
7. Факс*_____8. E-mail*_____
9. Сведения о владельце ключа
Фамилия, имя, отчество _____
Должность _____
Документ, удостоверяющий личность _____
серия _____ номер _____ дата выдачи "____ _____года
кем выдан _____
10. Примечания*_____
* необязательно для заполнения
Настоящим подтверждаю согласие на обработку банком м[illegible] персональных данных _____/
подпись

Ключ проверки [illegible]отрудника клиента
Идентификатор ключа проверки ЭП _____ Идентификатор токена _____
Наименование криптосредств _____
Алгоритм _____ ID набора па[illegible]етров алгоритма _____
Дата начала действия "____" _____20___г. (заполняется банком)
Дата окончания действия "____" _____ 20___г. (заполняется банком)
Представление ключа провер[illegible]шес[illegible]терично[illegible]м виде

Личная подпись владельца ключа проверки ЭП

Сертификат к[illegible]оч[illegible] провер[illegible]ЭП кли[illegible]та действует в рамках Договора на обслуживание в системе "iBank 2"
№_____ от __ _____ 20__г.

Группа п[illegible]ди[illegible] _____
(указать соответст[illegible] с должностью сотрудника, владельца ключа ЭП)

Достовер[illegible]сть пр[illegible]веденных данных подтверждаю

Руководитель организации
_____ / _____/
подпись Ф.И.О.

Уполномоченный представитель банка
_____ _____ / _____/
подпись Ф.И.О.

Оттиск печати

Оттиск печати

Дата приема сертификата ключа проверки ЭП
"__" _____ 20__ г.

Администратор безопасности системы.

_____ _____ / _____/
подпись Ф.И.О.

Оттиск печати

Дата регистрации сертификата ключа проверки ЭП
"__" _____ 20__ г.

БАНК _____ _____ КЛИЕНТ _____

Приложение № 5
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от **г.**

УВЕДОМЛЕНИЕ
О ПРЕКРАЩЕНИИ (ПРИОСТАНОВЛЕНИИ) ДЕЙСТВИЯ КЛЮЧА ПРОВЕРКИ ЭП КЛИЕНТА И СООТВЕТСТВУЮЩЕГО ЕМУ КЛЮЧА ЭП КЛИЕНТА

Клиент уведомляет Банк о том, что с «___»_____20__г. следует считать недействительным / следует заблокировать (ненужное зачеркнуть) Ключ проверки ЭП Клиента, имеющий идентификатор: _____, и соответствующий ему Ключ ЭП Клиента.

от Банка: от Клиента:

_____/ / _____/ /

М.П. М.П.

Уведомление принял и проверил: **ОТМЕТКИ БАНКА**

_____ _____ /_____/_____

(должность работника Банка) (ФИО) (Подпись) (Дата)

БАНК _____ _____ КЛИЕНТ _____

Приложение № 6
К договору по обслуживанию клиентов
по системе интернет банк
ЗАО «КОШЕЛЕВ-БАНК»
№ от «___»_____20___г.

ПАМЯТКА
КЛИЕНТУ О ВОЗМОЖНЫХ УГРОЗАХ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ СО СЧЕТОВ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ «IBANK 2» И СПОСОБАХ ЗАЩИТЫ

1. Настоящей Памяткой Банк информирует Вас о возможных случаях хищения денежных средств с Ваших банковских счетов при использовании Системы «iBank 2», мерах соблюдения безопасности и способах пресечения данного хищения.

2. Хищение денежных средств с расчетных счетов возможно при получении злоумышленниками тем или иным образом доступа к Ключам ЭП Клиента и паролям с целью направления в Банк платежных поручений, заверенных от Вашего лица похищенным Ключом электронной подписи, что предположительно могут осуществить:

- ответственные сотрудники Вашей Компании, ранее имевшие доступ к Ключам ЭП для Системы «iBank 2», например: уволенные директора, бухгалтеры и их заместители, а также совладельцы Компании;
- штатные ИТ-сотрудники Вашей Компании, имеющие или имевшие ранее технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с Ключами ЭП, а также доступ к компьютерам Компании, с которых осуществлялась работа по Системе «iBank 2»;
- нештатные, приходящие по вызову, ИТ-специалисты, обслуживающие компьютеры Вашей омпании, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого программного обеспечения на компьютеры, с которых осуществлялась или осуществляется работа по Системе «iBank 2»;
- другие злоумышленники путем заражения через Интернет Ваших компьютеров вредоносными программами, используя уязвимости системного и прикладного программного обеспечения (операционные системы, Web-браузеры, почтовые клиенты и пр.) с последующим дистанционным похищением Ключей ЭП и паролей.

3. Таким образом, в Банк могут поступать не вызывающие подозрений платежи, направленные злоумышленниками с использованием корректных и действующих Ключей ЭП Клиента, имеющие вполне обычные реквизиты получателей и типовые назначения платежа. И правомерное, в данном случае, исполнение таких платежей Банком приведёт к хищению денежных средств с Вашего Счета.

4. Важно понимать, что Банк не имеет доступа к Вашим Ключам ЭП и не может от Вашего имени сформировать Корректную ЭП Клиента под Электронным документом.

5. Вся ответственность за конфиденциальность Ваших Ключей ЭП полностью лежит на Вас, как единственных владельцах указанных Ключей.

6. Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать Ключ ЭП Клиента или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

7. Если Вы сомневаетесь в конфиденциальности своих Ключей ЭП или есть подозрение в их компрометации (копировании), Вы должны заблокировать свои Ключи ЭП.

8. Изменение пароля доступа к ключу ЭП не защищает от использования злоумышленником ранее похищенного Ключа.

9. Банк настоящим еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования Ключей ЭП и о необходимости ограничения доступа к персональным компьютерам, с которых осуществляется работа по Системе «iBank 2».

10. Чтобы воспрепятствовать хищению и использованию Вашего Ключа ЭП злоумышленниками, требуется придерживаться приведенных ниже правил и рекомендаций:

- использовать для работы с Ключами ЭП специализированные устройства – USB-токены «iBank 2 Key» (см. ниже);
- отключать, извлекать носители с Ключами ЭП, если они не используются для работы с Системой «iBank 2»;
- выделить отдельный компьютер, который использовать только для работы с Системой «iBank 2» и никакие другие задачи на этом компьютере не выполнять;
- ограничить доступ к компьютерам, используемым для работы с Системой «iBank 2»;
- исключить доступ к компьютерам персонала, не имеющего отношения к работе с Системой «iBank 2»;
- на компьютерах, используемых для работы с Системой «iBank 2», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения и т. п.;
- перейти к использованию лицензионного программного обеспечения (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного программного обеспечения;
- применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз;

БАНК _____ _____ КЛИЕНТ _____

● применять на рабочем месте специализированные программные средства безопасности: персональные файрволы, антишпионское программное обеспечение и т.п.;

● исключить обслуживание компьютеров, используемых для работы с Системой «iBank 2», нелояльными ИТ-сотрудниками;

● при обслуживании компьютера ИТ-сотрудниками – обеспечивать контроль за выполняемыми ими действиями;

● никогда не передавать Ключи ЭП ИТ-сотрудникам для проверки работы Системы «iBank 2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично Владелец сертификата ключа проверки ЭП сотрудника Клиента должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа «iBank 2», и лично ввести пароль, исключая подсматривание посторонними лицами;

● при увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно заблокировать его Ключ ЭП Клиента ;

● при увольнении сотрудника, имевшего технический доступ к ключу ЭП, обязательно заблокировать Ключ ЭП Клиента ;

● при увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с Системой «iBank 2», принять меры для обеспечения отсутствия вредоносных программ на компьютерах;

● при возникновении любых подозрений на компрометацию (копирование) Ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно заблокировать Ключи ЭП;

● если Вы заметили проявление необычного поведения программного обеспечения Системы «iBank 2» или какие-то изменения в интерфейсе программы – позвонить в Банк и выяснить, не связаны ли такие изменения с обновлением версии программного обеспечения. Если нет – заблокировать Ключи ЭП.

11. Чтобы исключить угрозу ХИЩЕНИЯ Ключей ЭП, а соответственно существенно повысить уровень безопасности при работе с Системой, необходимо использовать для генерации и хранения ключей ЭП специализированные устройства – USB-токены «iBank 2 Key».

12. При использовании «iBank 2 Key» Ключ ЭП Клиента генерируется самим USB-токеном при инициализации. Ключ ЭП Клиента используется только самим USB-токеном, хранится в защищенной памяти USB-токена и никогда, никем и ни при каких условиях не может быть считан из токена.

13. На вход USB-токена передается Электронный документ, а на выходе – сформированная USB-токеном ЭП под документом.

14. Важно понимать: использование USB-токена НЕ МОЖЕТ предотвратить хищение денежных средств с Вашего Счета в случае, если злоумышленникам удалось организовать (например, с использованием вредоносного программного обеспечения) удаленное управление компьютером, который используются для работы с Системой «iBank 2».

15. Повысить безопасность работы в Системе поможет также сервис электронного оповещения Системы «iBank 2».

16. Сервис электронного оповещения позволяет организовать рассылку сообщений (о входе в Систему, о движении средств по счёту и пр.) по каналам связи: SMS, e-mail.

17. Использование услуги электронного оповещения Системы «iBank 2» позволяет Вам самостоятельно настроить адреса и телефоны для автоматических, оперативных оповещений.

18. Если Вы получили уведомление о совершении данных действий от имени Вашей Компании, но ни Вы, ни Ваши сотрудники не совершали этих действий – необходимо срочно связаться с Банком и заблокировать Ключи ЭП.

19. Подтверждение платежных документов с помощью разовых SMS-паролей, является дополнительным механизмом защиты, при котором после подписи в Системе платежный документ получает статус «Требует подтверждения». Клиенту необходимо ввести разовый пароль, полученный в SMS-сообщении. SMS-сообщение с разовым паролем содержит также критичные реквизиты подтверждаемого платежа: сумму, наименование получателя, счет получателя, БИК банка получателя. Одним паролем могут быть подтверждены сразу несколько платежных поручений.

20. SMS-сообщение с разовым паролем поступает на телефонные номера лиц, уполномоченных Клиентом на проведение операций в Системе. Данные телефонные номера указываются Клиентом в соответствующем заявлении.

21. Все сообщения, которыми обмениваются серверный модуль с SMS-центрами российских сотовых операторов, подписываются электронными подписями и для обеспечения целостности передаваемых данных шифруются.

22. У Банка существует возможность разрешить каждому Клиенту работать только с заданных для данного Клиента IP-адресов и IP-подсетей. Список разрешенных IP-адресов и IP-подсетей задается в индивидуальных настройках клиента в банковском АРМе «Администратор» на основании поданного в Банк заявления Клиента. Однако, использование встроенного в систему «iBank 2» механизма IP-фильтрации ограничивает возможности Клиента работать с Системой при подключении к Интернету из произвольного места.

С настоящими Требованиями ознакомлен

Директор _____/_____/

подпись представителя Клиента

БАНК _____ _____ КЛИЕНТ _____

БАНК _____ _____ КЛИЕНТ _____