

**Положение  
об использовании системы «Интернет-Банк IBANK2»  
АКБ «Абсолют Банк» (ЗАО)  
Версия 4.0**

Оглавление

1	Общие положения и применяемые термины .....	3
2	Процедура генерации ключей и действия при их компрометации .....	5
3	Срок действия ключей .....	6
4	Хранение и использование ключей .....	6
5	Порядок работы в Системе и создания электронных документов Клиентом .....	6
6	Порядок передачи Клиентом и приема Банком электронных документов .....	7
7	Порядок разрешения споров .....	7
<u>      </u>	Приложение № 1 .....	10
<u>      </u>	Приложение № 2 .....	11

## 1 Общие положения и применяемые термины

1.1 Настоящее Положение о порядке использования системы «Интернет – Банк iBank2» АКБ «Абсолют Банк» (ЗАО) (далее по тексту – «Положение») определяет порядок обмена в электронном виде расчетными и иными документами между Акционерным коммерческим банком «Абсолют Банк» (закрытое акционерное общество) (далее по тексту – «Банк») и клиентами Банка – физическими лицами, юридическими лицами, индивидуальными предпринимателями и физическими лицами, занимающимися частной практикой (далее по тексту – «Клиент») при помощи системы «Интернет – Банк iBank2» на основании заключенных Договора о порядке обмена документами в электронном виде с использованием системы «Интернет – Банк iBank2», либо Договора о порядке обмена документами в электронном виде с использованием системы «Интернет – Банк iBank2» (с физическим лицом) (далее по тексту – «Договор»).

1.2 Термины, применяемые в Положении

1.2.1 Система «Интернет – Банк iBank2» (далее по тексту – «Система») – электронная банковская система, позволяющая Клиенту с использованием глобальной информационно-телекоммуникационной сети «Интернет» (далее по тексту – «Интернет») передавать в Банк в электронном виде расчетные и иные документы, отслеживать текущий статус этих документов, а также получать из Банка выписки по счетам, сообщения и иные документы.

1.2.2 Составляющими Системы являются:

- Центральный абонентский пункт Банка (далее по тексту – «ЦАП Банка») – сервер системы дистанционного банковского обслуживания, который обрабатывает всю передаваемую Клиентом в Банк информацию, а также размещает необходимую информацию на Интернет-сервере Системы;

- Абонентский пункт Клиента - оборудованный подсистемой защиты персональный компьютер Клиента, подсоединенный к Интернету, с которого Клиент осуществляет работу в Системе.

Абонентский пункт Клиента должен быть оборудован персональным компьютером, отвечающим следующим требованиям:

- цветной дисплей поддерживающий разрешение от 800x600 точек при шестнадцатибитном цвете;
- установленный и настроенный Интернет-браузер с поддержкой Java;
- настроенный канал доступа в Интернет.

1.2.3 *Электронные документы* – документы, в которых информация представлена в электронно-цифровом формате.

1.2.3.1 *Расчетный электронный документ* – расчетный документ в электронном виде, созданный Клиентом в Системе и оформленный в соответствии с требованиями действующего законодательства РФ.

1.2.3.2 *Иной электронный документ* – любой документ в электронном виде, кроме расчетного, созданный Клиентом или Банком в Системе.

1.2.4 *ЭЦП* – электронно-цифровая подпись - реквизит электронного документа, добавляемый к Электронному документу, полученный в результате криптографического преобразования информации, который позволяет получателю Электронного документа удостовериться в его авторстве и неизменности его содержания, в том числе в отсутствии подделки или искажения Электронного документа со стороны получателя или третьих лиц. Процедуры создания и проверки ЭЦП на базе асимметричного криптографического алгоритма с применением функции хэширования выполнены в соответствии с требованиями ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94.

1.2.5 *Ключ ЭЦП* (далее – «Ключ») – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всех возможных для данного алгоритма преобразований.

Ключ состоит из открытого и закрытого ключей, которые связаны между собой с помощью особого математического соотношения.

1.2.5.1 *Открытый ключ ЭЦП* – криптографический ключ (уникальная последовательность символов, соответствующая закрытому ключу ЭЦП), известный помимо Владельца ключа другим пользователям Системы и предназначенный для проверки подлинности ЭЦП. Открытый ключ ЭЦП позволяет установить авторство и неизменность содержания Электронного документа, но не позволяет вычислить закрытый ключ ЭЦП. Открытый ключ ЭЦП считается принадлежащим Клиенту, если такой ключ был

зарегистрирован в каталоге открытых ключей Центра регистрации ключей (далее по тексту «ЦРК») Банка в соответствии с порядком, установленным в разделе 2 Положения (Зарегистрированный ключ ЭЦП).

1.2.5.2 *Закрытый ключ ЭЦП* – криптографический ключ (уникальная последовательность символов), известный только Владельцу ключа (Клиенту или Банку соответственно) и хранимый Владельцем в тайне. Закрытый ключ ЭЦП используется для формирования ЭЦП.

1.2.6 *Каталог открытых ключей ЭЦП* – база данных Банка, элементами которой являются: наименования/ Ф.И.О. Клиентов - пользователей Системы, действующие открытые ключи ЭЦП Клиентов и идентификаторы открытых ключей ЭЦП Клиентов.

1.2.7 *Сертификат открытого ключа ЭЦП* – документ, содержащий информацию об открытом ключе ЭЦП Клиента: собственно открытый ключ ЭЦП и его идентификатор.

Сертификаты открытого ключа ЭЦП оформляются по форме, указанной в Приложении № 1 к Положению, подписываются Клиентом (уполномоченным лицом Клиента) и заверяются его печатью (при наличии). По одному экземпляру сертификата открытого ключа ЭЦП хранится в Банке и у Клиента.

1.2.8 *Компрометация ключа* – событие, связанное с утратой доверия к тому, что используемые ключи обеспечивают возможность установления авторства и неизменности содержания Электронного документа. К таким событиям относятся в том числе:

- утрата носителей информации с ключами;
- утрата носителей информации с ключами с последующим обнаружением;
- увольнение сотрудников Клиента-юридического лица, имевших доступ к закрытым ключам,

и иные события, в результате которых используемый ключ в целом или его часть (открытый либо закрытый ключи) могут стать известны или доступны третьим лицам, не уполномоченным на пользование ими.

1.2.9 *Блокировочное слово* - слово, которое Клиент указывает при первоначальной регистрации на сайте Банка, запоминает и использует в качестве пароля при обращении по телефону в Банк для временного блокирования работы Клиента в Системе в случае компрометации ключа ЭЦП.

1.2.10 *USB-токен «iBank 2 Key»* — аппаратное USB-устройство генерации и хранения ключей ЭЦП, состоящее из PC/SC-совместимого USB-картридера и SIM-карты, в которой реализованы все российские криптоалгоритмы и имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭЦП.

1.2.11 *Статус Электронного документа* – состояние Электронного документа в базе данных ЦАП Банка, однозначно соответствующее стадии обработки документа в Банке.

1.2.12 *Инструкция на проведение операции с Электронным документом* – команда, посылаемая Клиентом по Системе для изменения статуса Электронного документа.

1.2.13 *Владелец ключа ЭЦП Клиента* – уполномоченное лицо Клиента, осуществляющее от имени Клиента работу в Системе, на имя которого оформлен Сертификат открытого ключа ЭЦП, и которое владеет соответствующим закрытым ключом ЭЦП.

Владелец ключа ЭЦП должен отвечать следующим требованиям:

- обладает правом подписи расчетных документов,
- указан в карточке с образцами подписей и оттиска печати Клиента.

Если в действующей карточке с образцами подписей и оттиска печати указаны лица, обладающие второй подписью, то владельцев ключей ЭЦП Клиента должно быть не менее двух – по одному с первой и второй группой подписи.

1.2.13.1 *Функции Владельцев ключей ЭЦП Клиента:*

- заверение Электронных документов ЭЦП при помощи ключей;
- ответственное хранение ключей;
- своевременное извещение Банка о случаях компрометации ключей;
- контроль за соблюдением Клиентом при работе с Абонентского пункта Клиента установленных процедур работы в Системе;

- контроль за своевременностью обновления ключей по требованию Банка;
- организация регулярных сеансов связи с Банком (не реже одного раза в неделю) для своевременного получения из Банка выписок и служебных сообщений, а также иной информации, в т.ч. о текущем состоянии Электронных документов;

- осуществление регулярного просмотра корреспонденции в Системе.

1.3 От имени Банка работу в Системе осуществляют:

- Администратор ЦРК Банка;
- Администратор ЦАП Банка.

1.4 Клиент – юридическое лицо, физическое лицо, занимающееся частной практикой, индивидуальный предприниматель вправе ограничить список IP адресов, с которых Клиентом будет осуществляться доступ к Системе, путем заключения с Банком Соглашения об IP фильтрации по форме Приложения № 2 к Положению.

## **2 Процедура генерации ключей и действия при их компрометации**

2.1 Процесс генерации ключей осуществляется Клиентом, на персональном компьютере Клиента с использованием *USB-токена «iBank 2 Key»*. Полученные в ходе генерации сертификаты открытых ключей ЭЦП Клиента подписываются и передаются Клиентом в Банк на бумажном носителе.

2.2 Регистрация открытых ключей ЭЦП Клиента в Каталоге открытых ключей осуществляется Администратором ЦРК Банка не позднее, чем на следующий рабочий день после передачи Клиентом в Банк подписанных сертификатов открытых ключей ЭЦП, при условии соблюдения Клиентом требований п.1.2.13 Положения и корректного заполнения сертификатов.

2.3 Плановая регенерация ключей производится по истечении срока действия ключа согласно п.3.1 Положения или по инициативе любой из Сторон.

2.4 Если плановая регенерация ключей производится по инициативе Банка, Банк обязан проинформировать об этом Клиента по Системе за одну неделю до предполагаемой даты регенерации. С указанной Банком даты прежние ключи Клиента считаются недействительными.

2.5 Если плановая регенерация ключей производится по инициативе Клиента, Клиент обязан проинформировать об этом Банк по Системе за одну неделю до предполагаемой даты регенерации. При этом прежние ключи Клиента независимо от факта регенерации считаются недействительными с даты и времени, указанных Клиентом в соответствующем сообщении.

2.6 При компрометации ключа Клиент немедленно сообщает об этом Администратору ЦРК Банка (с учетом установленного режима работы - с понедельника по пятницу с 8-00 ч до 19-00 ч московского времени):

- при личной явке Клиента (уполномоченного представителя Клиента) в Банк путем предоставления письменного сообщения, заверенного подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке, или

- по телефону, используя блокировочное слово, с последующим предоставлением в Банк письменного сообщения, заверенного подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке.

ЦРК Банка фиксирует факт компрометации ключа, и Банк временно блокирует работу Клиента в Системе.

По письменному требованию Клиента, заверенному подписями уполномоченных лиц и оттиском печати (при наличии), указанными в карточке, Банк отменяет исполнение Расчетных электронных документов, принятых к исполнению до момента поступления заявления о компрометации, если Банк имеет технологическую возможность такой отмены.

Регенерация ключей производится Клиентом в соответствии с п.п. 2.1, 2.2 Положения.

2.7 Банк вправе блокировать работу Клиента в Системе при наличии подозрений в компрометации ключа Клиента без уведомления последнего. Возобновление работы Клиента происходит после регенерации Ключа в соответствии с п.п. 2.1, 2.2 Положения.

2.8 Исключение открытых ключей ЭЦП Клиента из Каталога открытых ключей ЦРК Банка производится на основании прекращения действия Договора, а также в случаях регенерации ключей.

2.9 После исключения открытых ключей ЭЦП Клиента из Каталога открытых ключей ЦРК Банка сертификаты открытых ключей ЭЦП Клиента хранятся в Банке не менее пяти лет.

### **3 Срок действия ключей<sup>1</sup>**

3.1 Срок действия ключа ЭЦП определяется сроком полномочий Владельца ключа распоряжаться средствами на счете Клиента с правом первой или второй подписи, но не превышает 1 (Один) год с даты начала действия ключа.

3.2 Банк уведомляет Владельца ключа о предстоящем истечении срока действия ключа по Системе за 30 календарных дней до даты окончания срока.

3.3 По окончании срока действия ключи подлежат обязательной регенерации Клиентом в соответствии с п.п. 2.1, 2.2 Положения, при этом прежние ключи Клиента, по которым истек срок действия, считаются недействительными с даты, следующей за датой окончания срока их действия.

### **4 Хранение и использование ключей**

4.1 Способ хранения Клиентом закрытых ключей и паролей к ключам должен исключать утрату и использование неуполномоченными лицами. Клиент обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение закрытых ключей.

4.2 В ЦРК Банка хранятся только открытые ключи Клиента. Закрытые ключи Клиента третьим лицам и Банку не известны.

4.3 Ответственность за все возможные последствия использования ключей Клиента неуполномоченными лицами несет Клиент.

### **5 Порядок работы в Системе и создания электронных документов Клиентом**

5.1 Инициатором передачи Расчетных электронных документов в Банк, а также получения от Банка информации, переданной по Системе, является Клиент. Для получения по Системе от Банка интересующей его информации Клиент формирует соответствующие Интернет-запросы, в ответ на которые Банк предоставляет запрашиваемую информацию.

5.2 Клиент самостоятельно устанавливает соединение с Интернет-сервером Системы и следит за поддержанием сеанса связи во время работы в Системе.

5.3 После осуществленной Системой идентификации Клиента последний получает доступ к Системе и начинает работу в ней.

5.4 Клиент заполняет или редактирует формы Электронных документов в формате, определенном в экранной форме клиентской части Системы, и заверяет созданные Электронные документы своей (своими) ЭЦП. ЭЦП подтверждает авторство созданного в Системе Электронного документа и является средством проверки неизменности его содержания, так как любое изменение Электронного документа после заверения его ЭЦП нарушает целостность ЭЦП.

Электронный документ должен быть заверен ЭЦП в строгом соответствии с действующей карточкой с образцами подписей и оттиска печати:

- при наличии лиц, обладающих правом второй подписи, документ заверяется двумя ЭЦП - по одной ЭЦП из первой и второй группы подписей.

5.5 Система автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком Электронного документа посредством присвоения Электронному документу определенного статуса в Системе.

Система присваивает Электронным документам следующие статусы:

- «новый»: присваивается вновь созданному в Системе Электронному документу;

- «подписан»: присваивается Электронному документу, заверенному необходимым количеством ЭЦП Клиента (по одной ЭЦП из каждой группы подписей, указанной в карточке с образцами подписей и оттиска печати);

---

<sup>1</sup> данный раздел распространяется на Клиентов – юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся частной практикой.

- «доставлен»: присваивается Электронному документу, успешно прошедшему проверку в соответствии с п. 6.2 Положения;
- «отвергнут»: присваивается Электронному документу, не прошедшему проверку в соответствии с п. 6.2 Положения, либо последующую проверку по причине его несоответствия требованиям, установленным действующим законодательством РФ или Положением, по причине недостаточности денежных средств на соответствующем счете Клиента, а также в иных случаях на усмотрение Банка;
- «на исполнении»: присваивается Расчетному электронному документу, находящемуся на этапе исполнения Банком;
- «на обработке»: присваивается Расчетному электронному документу, исполнение которого требует дополнительного контроля со стороны Банка;
- «проведен»: присваивается Расчетному электронному документу – после получения Банком выписки по соответствующему корреспондентскому счету Банка, подтверждающей исполнение такого документа, – если платеж исполнялся через корреспондентский счет, и непосредственно после отражения документа в балансе Банка – если платеж был исполнен внутри Банка.

5.6 Банк передает Клиенту по Системе следующие виды Электронных документов:

- выписки по счетам Клиента;
- расшифровки поступлений по счетам Клиента (кредитовые расчетные документы);
- справочную и иную информацию (в том числе формы учета по валютным операциям и документы, подтверждающие операции торгового финансирования и сделки на срочном рынке).

5.7 Информация, переданная Банком Клиенту по Системе, считается доведенной до сведения Клиента по истечении одной недели с даты ее передачи Банком (начиная со дня передачи), независимо от фактического восприятия такой информации Клиентом.

5.8 Все справочники, шаблоны Электронных документов, Электронные документы после их сохранения, а также выписки по счетам и иная информация находятся в ЦАП Банка и доступны Клиенту только во время проведения авторизованных сеансов связи с Банком по Системе.

## **6 Порядок передачи Клиентом и приема Банком электронных документов**

6.1 Созданный Клиентом Электронный документ может быть передан Клиентом в Банк по Системе как вместе с инструкцией на его исполнение, так и без такой инструкции.

При получении Банком инструкции на исполнение Электронного документа Банк осуществляет проверку Электронного документа и принимает его к исполнению при условии положительного результата проверки.

6.2 Результат проверки Электронного документа считается положительным, если Электронный документ оформлен в соответствии с действующим законодательством РФ и требованиями, установленными Положением, заверен надлежащей (надлежащими) ЭЦП и прошел в Банке проверку ЭЦП.

6.3 После проверки Банком Электронного документа Система присваивает ему статус «доставлен» или «отвергнут» соответственно.

Статус каждого Электронного документа, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами ЦАП Банка во время сеансов связи, проводимых Клиентом. Свидетельством того, что Электронный документ принят к исполнению Банком, является присвоение ему в Системе статуса «доставлен».

6.4 Информация об Электронных документах, не принятых Банком к исполнению по причине их оформления с нарушением требований п. 6.2 Положения или по иным основаниям, размещается Банком на Интернет-сервере Системы в течение рабочего дня (с учетом установленного режима работы Банка), следующего за днем получения инструкции на исполнение Электронного документа, с указанием причины, по которой документ не принят к исполнению.

## **7 Порядок разрешения споров**

7.1 Стороны в рабочем порядке урегулируют все споры, возникающие между ними в ходе работы в Системе, за исключением споров, указанных в п. 7.2 Положения.

7.2 Споры Сторон по поводу авторства и неизменности содержания Электронных документов рассматриваются Экспертной комиссией, формируемой сторонами (далее по тексту – «Комиссия»). Процедура рассмотрения спора состоит из следующих этапов:

- предъявление претензии одной из Сторон другой Стороне;
- формирование Комиссии для рассмотрения спора;
- разрешение Комиссией спора по существу.

7.3 Претензия предъявляется соответствующей Стороной в письменной форме путем официального вручения под расписку другой Стороне или направления по почте телеграммой либо заказным письмом с уведомлением о вручении.

7.4 Получив претензию, соответствующая Сторона официально в письменной форме информирует другую Сторону о результатах ее рассмотрения в течение 5 (Пяти) рабочих дней с даты получения претензии.

7.5 Сторона, предъявившая претензию, в течение 5 (Пяти) рабочих дней после получения результатов рассмотрения претензии от другой Стороны должна рассмотреть представленные объяснения и письменно уведомить другую Сторону о снятии претензии или о несогласии с представленными объяснениями.

7.6 Если Сторона не согласна с представленными объяснениями, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты уведомления о несогласии сформировать Комиссию для рассмотрения и разрешения указанного спора по существу.

7.7 До передачи спора на рассмотрение Комиссии Сторонам следует удостовериться, что причиной возникновения спора не является нарушение целостности программного обеспечения, произошедшее в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет, и т.п. В этом случае Стороны руководствуются п. 7.1 Положения.

7.8 В состав Комиссии включается равное количество представителей Банка и Клиента. При необходимости в состав Комиссии могут быть включены независимые эксперты, в частности, представители компании - разработчика Системы. Максимальное количество членов Комиссии не должно превышать 6 (Шести) человек.

7.9 Полномочия представителей Сторон для участия в Комиссии должны подтверждаться оформленными надлежащим образом доверенностями.

7.10 Заседание Комиссии проводится не позднее 2 (Двух) рабочих дней со дня ее формирования.

7.11 При рассмотрении спора об авторстве и неизменности содержания Электронного документа Комиссия устанавливает следующие факты:

- предмет спора Сторон;
- перечень Электронных документов, относящихся к предмету спора;
- идентичность созданного Клиентом Электронного документа документу на бумажном носителе, распечатанному Банком и хранимому в документах дня Банка;
- принадлежность ЭЦП Электронного документа Клиенту.

7.12 При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:

- данные имеющегося в Банке архива отправленных/принятых Электронных документов;
- сертификат(ы) открытого ключа ЭЦП Клиента, подписанный(ые) Клиентом и хранящийся (хранящиеся) в Банке (Эталонный(е) сертификат(ы)).

7.13 Разрешение споров осуществляется на основании результатов проверки ЭЦП Клиента в спорном Электронном документе.

7.14 Комиссия осуществляет свою работу на территории Банка с использованием персонального компьютера, свободного от вирусов и программных закладок, с установленными на нем эталонными DLL-библиотеками СКЗИ, предоставляемыми ООО «БИФИТ».

7.15 Для рассмотрения спора Комиссией Администратор ЦРК Банка предоставляет Эталонный(е) сертификат(ы).

7.16 Клиент для рассмотрения спора Комиссией предоставляет сертификат(ы) открытого ключа ЭЦП Клиента, хранящийся (хранящиеся) у Клиента.

7.17 Если инициатором рассмотрения спора является Клиент, Комиссией устанавливается актуальность открытых ключей ЭЦП Клиента на момент передачи Электронного документа, являющегося объектом спора. Открытые ключи ЭЦП Клиента считаются актуальными, если они были зарегистрированы в Каталоге открытых ключей в соответствии с п. 2.2 Положения и действовали в момент, когда спорный Электронный документ был передан Клиентом в Банк.

7.18 Принимая во внимание математические свойства алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения сертифицированной ЭЦП любым лицом, не обладающим закрытым ключом ЭЦП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания Электронного документа заключается в доказательстве принадлежности ЭЦП конкретного Электронного документа конкретной Стороне.

7.19 Рассмотрение Комиссией спора об авторстве и неизменности содержания Электронного документа проводится с использованием АРМ «Операционист» Системы «iBank2».

7.20 В целях формирования Протокола проверки ЭЦП Администратор ЦАП Банка в присутствии Комиссии осуществляет следующие действия:

- выводит на печать сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей, используя АРМ «Администратор» Системы «iBank2»;

- сравнивает распечатанный сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей с Эталонным сертификатом, предоставленным Комиссии Администратором ЦРК Банка, а также с аналогичным сертификатом, хранящимся у Клиента и представленным Комиссии Клиентом.

Значения открытого ключа ЭЦП Клиента, содержащиеся в Каталоге открытых ключей, в Эталонном сертификате и в хранящемся у Клиента сертификате, должны совпасть. В случае их несовпадения верным признается Эталонный сертификат;

- с помощью АРМ «Операционист» находит спорный документ и, используя меню «Проверить ЭЦП», формирует результат проверки ЭЦП, в котором указываются идентификаторы ключей ЭЦП, участвовавшие в подписи документа, авторство которого оспаривается;

- выводит на печать Документ со списком идентификаторов подписавших его ключей ЭЦП.

В случае, если спорный Электронный документ был подписан несколькими ЭЦП, данная процедура повторяется применительно к каждой ЭЦП.

7.21 Принадлежность ЭЦП Клиенту и авторство Электронного документа считается установленным, если идентификаторы открытых ключей ЭЦП, содержащихся в списке идентификаторов, подписавших Документ, и Эталонном сертификате совпадают, в Документе сформирована запись «ЭЦП Корректна», и распечатанный сертификат открытого ключа ЭЦП Клиента из Каталога открытых ключей совпадает с Эталонным сертификатом.

7.22 Заключение Комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон - и подписывается всеми членами Комиссии.

7.23 Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.

7.24 Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с Заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда в соответствии с Положением Комиссия должна быть создана, возникший спор передается на рассмотрение и разрешение по существу суду, определенному Сторонами в Договоре.

Все иные споры Сторон, связанные с обменом Электронными документами по Системе, также передаются на рассмотрение указанного в настоящем пункте суда.

**Сертификат открытого ключа ЭЦП Клиента в системе «Интернет-Банк iBANK2»  
АКБ «Абсолют Банк» (ЗАО)**

- 1 Наименование / ФИО Клиента \_\_\_\_\_  
2 Местонахождение / адрес регистрации по месту жительства Клиента \_\_\_\_\_  
3 Почтовый адрес Клиента \_\_\_\_\_  
4 Наименование документа о регистрации, кем и когда выдан \_\_\_\_\_  
5 Тел. \_\_\_\_\_ 6 ИНН \_\_\_\_\_ 7 КПП \_\_\_\_\_  
8 Факс \_\_\_\_\_ 9 E-mail \_\_\_\_\_  
10 Сведения о владельце открытого ключа ЭЦП  
Фамилия, Имя, Отчество \_\_\_\_\_  
Должность \_\_\_\_\_  
Документ, удостоверяющий личность \_\_\_\_\_, серия \_\_\_\_\_, номер \_\_\_\_\_  
кем выдан \_\_\_\_\_  
\_\_\_\_\_ дата выдачи «\_\_» \_\_\_\_\_ года.  
11 Примечания \_\_\_\_\_

**Открытый ключ ЭЦП клиента**

Идентификатор \_\_\_\_\_

Дата начала действия «\_\_» \_\_\_\_\_ 200\_\_ г.

Дата окончания действия «\_\_» \_\_\_\_\_ 200\_\_ г.

Представление открытого ключа ЭЦП в шестнадцатиричном виде:

FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Группа подписи \_\_\_\_\_

Сертификат открытого ключа ЭЦП клиента в системе Интернет Банк iBank2 действует в рамках договора на обслуживание в системе Интернет Банк iBank2 № \_\_\_\_\_ от \_\_\_\_\_ 200\_\_ г.

**Достоверность приведенных данных подтверждаю**

Личная подпись владельца ЭЦП

Руководитель организации

Уполномоченный представитель Банка

\_\_\_\_\_

\_\_\_\_\_

Оттиск печати

Оттиск печати  
Банка

**Соглашение об IP фильтрации**

г. \_\_\_\_\_ «\_\_» \_\_\_\_\_ 200\_\_ года

**Акционерный коммерческий банк «Абсолют Банк» (закрытое акционерное общество),**  
именуемый в дальнейшем «**Банк**», в лице \_\_\_\_\_

действующего на основании доверенности от «\_\_» \_\_\_\_\_ 200\_\_ года № \_\_\_\_\_, с одной стороны,  
и \_\_\_\_\_

*(Полное фирменное наименование Клиента)*

именуем \_\_\_\_\_ в дальнейшем «**Клиент**», в лице \_\_\_\_\_, действующего на основании \_\_\_\_\_, с другой стороны,  
заключили настоящее соглашение (далее по тексту – «Соглашение») о нижеследующем:

1 Разрешить Клиенту доступ к системе «Интернет-Банк iBank2» только со следующих IP адресов:

№ п/п	IP адрес			
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

2 Соглашение действует в рамках договора на обслуживание в системе Интернет Банк iBank2 № \_\_\_\_\_ от \_\_\_\_\_ 200\_\_ г. (далее по тексту – Договор) и утрачивает силу при заключении нового соглашения о IP-фильтрации или расторжении Договора.

3 Настоящее соглашение составлено в двух экземплярах – по одному для каждой из Сторон, и считается действительным при наличии подписей Сторон и печати Банка.

**Место нахождения и реквизиты сторон**

**Реквизиты Банка:**

Акционерный коммерческий банк «Абсолют Банк» (закрытое акционерное общество).

Место нахождения: 127051, г. Москва, Цветной бульвар, д. 18.

Место нахождения Филиала: \_\_\_\_\_ (указывать только филиалам)

Кор. счет: \_\_\_\_\_, БИК \_\_\_\_\_ ИНН 7736046991.

Счет в долларах США (USD) - № 18301701 with KBC BANK NV, 1177 Avenue of the Americas, New York, NY 10036, USA, SWIFT: KREDUS33;

Счет в Евро (EUR) - № 488591799660 with KBC BANK NV, B – 1080 Brussels, Belgium, SWIFT: KREDBEBB.

Absolut Bank, Moscow, Russia; SWIFT: ABSLRUMM.

Телефон: \_\_\_\_\_ . Факс: \_\_\_\_\_ .

**Реквизиты Клиента:**

Наименование: \_\_\_\_\_

Место нахождения: \_\_\_\_\_

ИНН, КПП, ОКПО: \_\_\_\_\_

Платежные реквизиты: \_\_\_\_\_

Телефон: \_\_\_\_\_

**Подписи сторон**

\_\_\_\_\_

\_\_\_\_\_ / \_\_\_\_\_ /

\_\_\_\_\_

\_\_\_\_\_ / \_\_\_\_\_ /