

УТВЕРЖДЕНО

**Правлением АКБ «ПЕРЕСВЕТ» (АО)
протокол от « 16 » апреля 2018 г.
№ 24**

Введено в действие с «28 » апреля 2018

ПРАВИЛА

**ПО ИСПОЛЬЗОВАНИЮ СИСТЕМЫ ДИСТАНЦИОННОГО
БАНКОВСКОГО ОБСЛУЖИВАНИЯ
BS-CLIENT V.3**

АКБ «ПЕРЕСВЕТ» (АО)

Регистрационный № _____

Версия 1.00

г. Москва 2018 г.

Оглавление:

1. Статус настоящих Правил	3
2. Сведения о Банке АКБ «ПЕРЕСВЕТ» (АО)	3
3. Используемые термины и понятия	4
4. Порядок заключения Соглашения по использованию Системы ДБО	5
4.1. Акцепт Правил	5
4.2. Регистрация Заявления Клиента	6
5. Предмет Соглашения об использовании Системы ДБО	7
6. Порядок подтверждения полномочий использования ЭП Клиента	7
7. Порядок проведения электронных расчетов	9
8. Права и обязанности сторон	11
8.1. Взаимные права и обязанности сторон	11
8.2. Права и обязанности Клиента	11
8.3. Права и обязанности Банка	12
9. Ответственность сторон	14
10. Финансовые взаимоотношения	15
11. Срок действия Соглашения	16
12. Изменение и дополнение Правил	17
13. Урегулирование претензий и рассмотрение споров Сторон	17
14. Обработка персональных данных	17
15. Заключительные положения	18
Приложение № 1	19
Приложение № 2	29
Приложение № 3	31
Приложение № 4	33
Приложение № 5	34
Приложение № 6	35
Приложение № 7	36
Приложение № 8	37
Приложение № 9	38

1. Статус настоящих Правил

1.1. Настоящие Правила Акционерного коммерческого банка содействия благотворительности и духовному развитию отечества «ПЕРЕСВЕТ» (Акционерное общество) по использованию Системы дистанционного банковского обслуживания BS-Client v.3 (далее – Правила) определяют условия, на которых Акционерный коммерческий банк содействия благотворительности и духовному развитию отечества «ПЕРЕСВЕТ» (Акционерное общество) (далее – АКБ «ПЕРЕСВЕТ» (АО), или Банк) оказывает юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой, резидентам и нерезидентам Российской Федерации услуги по использованию системы дистанционного банковского обслуживания BS-Client v.3 при осуществлении документооборота между клиентами и Банком в рамках договоров банковского счета, договоров об открытии и ведении корреспондентского счета/корреспондентского субсчета, заключенных между клиентами и Банком (далее по тексту – Договор банковского счета), или иных договоров, и иные сопутствующие услуги, перечень которых излагается в тексте Правил.

1.2. Опубликование Правил, включая распространение их текста, осуществляется через информационно-телекоммуникационную сеть Интернет на официальном сайте Банка. Банк адресует Правила всем заинтересованным лицам и рассматривает их опубликование (распространение) как публичное предложение (оферту) со стороны АКБ «ПЕРЕСВЕТ» (АО) заключить Соглашение об использовании Системы дистанционного банковского обслуживания BS-Client v.3 (далее – Соглашение).

1.3. Заинтересованные лица – юридические лица и индивидуальные предприниматели, физические лица, занимающиеся в установленном законодательством Российской Федерации порядке частной практикой, резиденты и нерезиденты Российской Федерации, заключившие (заключающие) с Банком Договоры банковского счета или иные договоры и Соглашение в порядке, определенном настоящими Правилами (далее по тексту - Клиенты).

1.4. На основании Соглашения Банк и Клиент (далее совместно – Стороны) осуществляют электронный документооборот в рамках Договоров банковского счета, а в случаях, установленных иными договорами – в рамках таких договоров.

1.5. Заключение Соглашения осуществляется путем совершения заинтересованным лицом письменного акцепта Правил. Акцепт Правил должен быть произведен путем передачи Банку Заявления на конфигурацию АРМ Системы дистанционного банковского обслуживания BS-Client v.3 (далее – Заявление Клиента, Заявление). Соглашение является неотъемлемой частью Договора банковского счета и/или иного договора.

2. Сведения о АКБ «ПЕРЕСВЕТ» (АО)

Полное наименование – Акционерный коммерческий банк содействия благотворительности и духовному развитию Отечества «ПЕРЕСВЕТ» (Акционерное общество).

Сокращенное наименование – АКБ «ПЕРЕСВЕТ» (АО).

Место нахождения: 123100, г. Москва Краснопресненская наб., дом 14.

Основной государственный регистрационный номер – 1027739250285.

Корреспондентский счет № 30101810145250000275 в Главном управлении Центрального банка Российской Федерации по Центральному федеральному округу г. Москва (ГУ Банка России по Центральному федеральному округу).

БИК - 044525275.

ИНН - 7703074601.

Официальный сайт Банка в информационно-телекоммуникационной сети Интернет - www.bank-peresvet.ru.

Лицензии:

1. Генеральная лицензия на осуществление банковских операций № 2110 выдана Центральным банком Российской Федерации 19 июня 2015 года.
2. Лицензия на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) ЛСЗ № 0007610 Per № 12609 Н от 07 декабря 2012 года, выдана Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.
3. Правообладателем программного обеспечения для ЭВМ «ДБО BS-Client» является ООО «Банк Софт Системс». Банк обладает неисключительным правом на распространение и использование программного обеспечения для ЭВМ «ДБО BS-Client» для оказания Банком банковских услуг третьим лицам в рамках лицензии.

Поддержка Клиентов осуществляется с 09:00 до 18:00 московского времени по рабочим дням. Единый Центр технической поддержки обслуживания Клиентов в объеме Правил осуществляется по телефону и электронной почте:

- (495) 229-43-62 для звонков по Москве,
- г. Санкт-Петербург (812) 275-92-66
- e-mail: bk@bank-peresvet.ru.

3. Используемые термины и понятия

- 3.1. **Система ДБО** - Система дистанционного банковского обслуживания BS-Client v.3, с использованием которой Клиент и Банк обмениваются электронными документами.
- 3.2. **Автоматизированное рабочее место (АРМ) Клиента (Абонентский пункт Клиента)** – программно-аппаратный комплекс, состоящий из оборудования, общесистемного программного обеспечения и программного обеспечения Системы ДБО в составе и в соответствии с требованиями, указанными в Приложении № 2 к Соглашению.
- 3.3. **Электронный документ (ЭД)** – документ в электронно-цифровой форме, обеспечивающий обмен информацией при взаимодействии Клиента и Банка с использованием Системы ДБО.
- 3.4. **Электронный платежный документ (ЭПД)** – надлежаще оформленный электронный документ, содержащий необходимое количество корректных Электронных подписей Клиента. ЭПД является основанием для совершения расчетных операций с использованием Системы ДБО и имеет равную юридическую силу с платежными документами на бумажном носителе, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

3.5. **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. Электронная подпись является видом аналога собственноручной подписи, предназначенным для защиты электронного документа от подделки и является обязательным реквизитом электронного документа. ЭП вырабатывается в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяет идентифицировать владельца ключа ЭП, а также установить отсутствие искажений информации в электронном документе с момента выработки ЭП. Каждый ключ ЭП в Системе ДБО закрепляется для использования за конкретным уполномоченным лицом Клиента, владельцем ключа ЭП. При этом считается, что ЭП используется от имени данного Клиента.

ЭП, используемая в рамках настоящих Правил, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» является усиленной неквалифицированной электронной подписью.

3.6. **Ключ электронной подписи (закрытый ключ)** - уникальная последовательность символов, предназначенная для создания электронной подписи. Закрытый ключ ЭП должен храниться в тайне.

3.7. **Ключ проверки электронной подписи (открытый ключ)** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. Открытый ключ должен быть доступен Клиенту.

3.8. **Криптографический профиль (профиль)** – запись в базе данных Системы ДБО, содержащая информацию о криптографических ключах Клиента.

3.9. **Компрометация ключа ЭП** – событие, определенное владельцем ключа ЭП, как создающее угрозу неправомерного использования закрытого ключа ЭП, в том числе, ознакомление неуполномоченного лица с закрытым ключом ЭП, его утрата, хищение.

3.10. **Счет** – банковский счет Клиента, открытый в Банке на основании Договора банковского счета.

3.11. **Карточка регистрации Ключа проверки электронной подписи (Карточка регистрации)** – электронный документ, изготовленный и подписанный ЭП ЦУКС Банка, подтверждающий принадлежность Ключа проверки электронной подписи владельцу и включающий в себя Ключ проверки электронной подписи Клиента, номер и срок действия Ключа проверки электронной подписи.

3.12. **Расчетные операции** – операции перевода денежных средств по Счетам, конверсионные операции, операции по обязательной продаже валюты.

4. Порядок заключения Соглашения по использованию Системы ДБО

4.1. Акцепт Правил

4.1.1. Заключение Соглашения об использовании Системы дистанционного банковского обслуживания BS-Client v.3 осуществляется путем совершения заинтересованным лицом письменного акцепта Правил. Акцепт Правил осуществляется путем направления (представления) Банку Заявления на конфигурирование АРМ Системы ДБО Клиента, составляемого по форме Приложения № 3 к Правилам, подписанного уполномоченными лицами Клиента. Акцепт будет считаться полным, безоговорочным и состоявшимся с момента регистрации Заявления Клиента в Банке в порядке, предусмотренном настоящим разделом Правил. Акцепт Правил является полным и безоговорочным.

4.1.2. Заявление Клиента может быть представлено уполномоченным представителем Клиента, в том числе курьером. При этом полномочия представителя Клиента, передающего в Банк Заявление Клиента, должны быть подтверждены доверенностью, оформленной надлежащим образом.

4.1.3. Заявление Клиента предоставляется в 1 (одном) подлинном экземпляре. При регистрации Заявления Банк изготавливает его копию и возвращает Клиенту с отметками о принятии и регистрации.

4.1.4. До заключения Соглашения Банк информирует Клиента об условиях и правилах работы в Системе ДБО, об использовании Ключа проверки электронной подписи, в том числе о случаях ограничения способов и мест его использования, о случаях повышенного риска использования Системы ДБО и Ключа проверки электронной подписи. Информирование Клиента осуществляется путем размещения информации и документов на официальном сайте Банка в информационно-телекоммуникационной сети Интернет, предоставление информации и документов Клиенту на бумажном носителе и в форме устных разъяснений. Подписание Клиентом Заявления подтверждает факт получения Клиентом всей необходимой информации.

4.2. Регистрация Заявления Клиента

4.2.1. Регистрация Заявления Клиента осуществляется при одновременном соблюдении следующих условий:

- соответствие Заявления Клиента требованиям Правил (при соответствии форме Приложения № 3 к Правилам);
- предоставление документов, указанных в п. 6.7. Правил;
- наличие действующего Договора банковского счета / иного договора, заключенного между Клиентом и Банком;
- на Счете достаточно денежных средств для списания комиссии Банка за подключение Системы ДБО (для Клиентов, которым открыт Счет в Банке), либо Клиентом иным способом оплачена комиссия Банка за подключение Системы ДБО (для Клиентов, которым Счет в Банке не открыт).

4.2.2. Регистрация Заявления Клиента осуществляется путем присвоения номера Заявлению и подписания уполномоченным лицом Банка. Номер Заявления и дата регистрации Заявления являются соответственно номером Соглашения и датой его заключения.

4.2.3. Банк вправе отказать в приеме и, соответственно, в регистрации Заявления Клиента и заключении Соглашения, в случае если:

- Заявление Клиента не соответствует форме Приложения № 3 к Правилам;
- между Клиентом и Банком отсутствует заключенный Договор банковского счета / иной договор;
- не предоставлены документы, указанные в п. 6.7. Правил;
- в случаях, установленных законодательством Российской Федерации;
- на Счете недостаточно денежных средств для оплаты комиссий Банка за подключение Системы ДБО (для Клиентов, которым открыт Счет в Банке), либо Клиентом не предварительно оплачена комиссия Банка за подключение Системы ДБО (для Клиентов, которым Счет в Банке не открыт).

4.2.4. С момента регистрации Заявления Клиента Соглашение об использовании Системы ДБО считается заключенным. Зарегистрированное Банком Заявление Клиента и утвержденные Банком Правила, составляют заключенное между Банком и Клиентом Соглашение об использовании Системы ДБО.

4.2.5. В случае если у Клиента возникнет необходимость внесения изменений в сведения, указанные в Заявлении, Клиент подает в Банк новое Заявление на конфигурирование АРМ Системы ДБО по форме Приложения № 3 к Правилам, в котором указываются все необходимые изменения. При регистрации Заявления Банк изготавливает его копию и возвращает Клиенту с отметкой о принятии. Зарегистрированное Заявление является дополнительным соглашением к Соглашению.

5. Предмет Соглашения об использовании Системы ДБО

5.1. Банк и Клиент устанавливают между собой порядок обмена Электронными документами в рамках Договора банковского счета / иного договора с использованием Системы ДБО.

Стороны устанавливают между собой порядок проведения расчетных операций по открытым Клиентом в Банке Счетам в электронной форме с использованием Системы ДБО.

5.2. Для проведения обмена электронными документами в Системе ДБО Клиент использует программное обеспечение, указанное в Приложении № 2 к Правилам (далее – программное обеспечение). Банк передает Клиенту неисключительные права на использование программного обеспечения на весь срок действия Соглашения. При прекращении Соглашения Клиент обязан удалить полученное от Банка программное обеспечение. Лицензии на программное обеспечение передаются в электронном виде.

5.3. Банк обслуживает Клиента по Системе ДБО на условиях настоящих Правил с момента подписания Сторонами двухстороннего Акта о начале использования Системы ДБО по форме Приложения № 6 к Правилам.

5.4. По Правилам Банк осуществляет расчетные операции по Счетам на основании распоряжений и иных документов, в электронном виде передаваемых в Банк по Системе ДБО, если таковые предусмотрены соответствующими договорами, заключенными с Клиентами, в рамках которых Клиенты подключены к Системе ДБО.

5.5. Стороны признают, что документ или распоряжение в электронном виде, подтвержденные Клиентом путем наложения на него корректной ЭП, либо двух таких подписей, юридически эквивалентны соответствующему документу или распоряжению на бумажном носителе с соответствующими подписями и печатями и является основанием для осуществления операций.

5.6. Стороны признают используемую ими по Правилам Систему ДБО, состоящую из подсистем обработки, хранения, защиты (в т.ч. криптографической) и передачи информации, достаточной для обеспечения надежной, эффективной и безопасной работы.

5.7. Стороны признают используемую ими по Правилам подсистему защиты информации достаточной для защиты от несанкционированного доступа, а также подтверждения авторства и подлинности электронного документа.

6. Порядок подтверждения полномочий использования ЭП Клиента

6.1. Использовать ЭП от имени Клиента имеет право физическое лицо, являющееся сотрудником Клиента, специально уполномоченное Клиентом на право распоряжения денежными средствами Клиента, находящимися на Счете, с использованием ЭП (далее по тексту - Уполномоченное лицо), о чём Банк уведомлен в предоставленном по форме Приложения № 3 к Правилам Заявлении.

6.2. Клиент по своему усмотрению может предоставить следующие права использования ЭП от своего имени:

- единственная ЭП – предоставляет право получать, создавать, заверять, визировать и отправлять в Банк на исполнение любые ЭД, обмен которыми разрешен в соответствии с настоящим Соглашением;
- ЭП группы А – предоставляет право получать, создавать, заверять и отправлять в Банк любые ЭД, обмен которыми разрешен в соответствии с настоящим Соглашением; исполнение отправленных документов Банком не производится до заверения ЭД ЭП группы Б;
- ЭП группы Б – предоставляет право получать, создавать, заверять и отправлять в Банк любые ЭД, обмен которыми разрешен в соответствии с настоящим Соглашением; исполнение отправленных документов Банком не производится без заверения ЭД ЭП группы А;
- ЭП без права подписи – предоставляет право получать, создавать любые ЭД, обмен которыми разрешен в соответствии с настоящим Соглашением; исполнение документов Банком не производится до заверения ЭД необходимыми подписями.

6.3. Использование ключа ЭП с правом единственной подписи исключает возможность использования Клиентом ключей ЭП группы А и ЭП группы Б.

6.4. Указанные выше права подписи не распространяются на предоставление в Банк электронного запроса на изготовление Карточки регистрации. Такие запросы всегда подписываются одним ключом ЭП. При этом процедура смены ключа предполагает замену ключа, с использованием которого подписан запрос на ключ, Карточка регистрации которого должна быть изготовлена в соответствии с данным запросом.

6.5. На каждый ключ ЭП оформляется отдельный Акт признания ключа проверки электронной подписи, который подписывается Уполномоченным лицом и руководителем Клиента, после чего заверяется печатью Клиента (при наличии).

6.6. При возникновении необходимости внесения изменений в права использования ЭП от имени Клиента оформляется Заявление по форме Приложения № 3 к Правилам, на основании которого изготавливаются новые комплекты ключей. При необходимости в Заявлении указываются изменения в составе и полномочиях Уполномоченных лиц.

6.7. Одновременно с заключением Соглашения Клиент обязан предоставить в Банк следующие документы для каждого Уполномоченного лица:

- копию документа, подтверждающего полномочия лица, наделенного правом использования ЭП от имени Клиента (такими документами могут быть Устав, доверенность или внутренний нормативно-распорядительный акт Клиента);
- копию документа, удостоверяющего личность Уполномоченного лица, а также копию миграционной карты и документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации;
- анкету на Уполномоченное лицо по форме, установленной Банком.

Если вышеуказанные документы были предоставлены в Банк ранее и являются действительными на день приема Заявления на конфигурирование АРМ Системы ДБО Клиента, повторное предоставление документов не требуется.

6.8. Копии документов заверяются Клиентом и должны содержать подпись лица, заверившего копию документа, его Ф.И.О. и должность, дата заверения, а также оттиск печати (при наличии) Клиента. Копии также могут быть изготовлены и заверены Банком в соответствии с установленным в Банке порядком. В случае заверения копий документов Клиентом, с копиями соответствующих документов в Банк предоставляются их оригиналы для проверки верности копий. Копии документов могут быть удостоверены нотариально.

6.9. Клиент имеет право в любое время отозвать полномочия любого Уполномоченного лица и наделить правом использования ЭП от имени Клиента иное лицо. В этом случае Клиент обязан своевременно уведомить о таком изменении Банк с предоставлением необходимых документов на каждое новое Уполномоченное лицо. На новое Уполномоченное лицо генерируется новый ключ ЭП.

6.10. В случае изменения каких-либо данных Уполномоченных лиц, либо увольнения Уполномоченных лиц, Клиент обязан незамедлительно уведомить о таком изменении Банк с предоставлением копий необходимых документов, указанных в п. 6.7. Правил (при изменении данных). Уведомление об изменениях данных Уполномоченных лиц без предоставления всех необходимых документов не считается надлежащим уведомлением.

6.11. Все риски, связанные с несвоевременным, ненадлежащим уведомлением Банка, либо с отсутствием уведомления несет Клиент.

7. Порядок проведения электронных расчетов

7.1 Клиентская часть Системы ДБО устанавливается на стороне Клиента и обеспечивает проведение расчетных операций и получение справочной информации.

7.2 Клиент определяет перечень устанавливаемых компонентов Системы ДБО и порядок их установки в момент подписания Заявления по форме Приложения № 3 к Правилам.

7.3 Проведение всех расчетных операций и получение всей информации по Системе ДБО осуществляется Клиентом с использованием публичных телекоммуникационных сетей.

7.4 Клиент оформляет ЭД, а также дает Банку распоряжение на его исполнение, путем генерации и присоединения к ЭД необходимого количества зарегистрированных Банком ЭП Клиента в соответствии с их назначением и осуществляет отправку ЭД в Банк. Банк осуществляет логическую проверку полученного ЭД и, в случае положительных результатов проверки, сохраняет его, а при наличии необходимого количества зарегистрированных ЭП Клиента соответствующего назначения, также осуществляет их проверку. К исполнению принимаются ЭД, прошедшие все проверки с положительным результатом.

7.5 Порядок передачи и приема ЭД установлен в Приложении № 1 к Правилам.

7.6 Банк при использовании Системы ДБО принимает ЭД, только если они соответствуют указанному ниже закрытому перечню распоряжений:

- Платежное поручение (расчетные (платежные) документы и/или Реестр платежей)
- Заявка на покупку валюты
- Заявка на продажу валюты
- Поручение на обязательную продажу валюты
- Запрос о подтверждении ЭПД
- Заявление на отзыв распоряжения с определенной стадии обработки
- Запрос на выпуск Карточки регистрации
- Паспорт сделки по контракту
- Паспорт сделки по кредитному договору
- Заявление о переоформлении паспорта сделки
- Заявление о закрытии/переводе паспорта сделки
- Справка о подтверждающих документах
- Справка о валютных операциях
- Запрос выписки
- Распоряжение на списание средств с транзитного валютного счета,

а также документы свободного формата, содержащие обрабатываемые Банком файлы, заявки и документы следующего назначения:

- Документы, подтверждающие вывоз/ввоз товара с/на территории Российской Федерации, а также выполнение работ, оказание услуг, передачу информации и результатов интеллектуальной деятельности, в том числе исключенных прав на них; исполнение (прекращение) обязательств иным способом, изменение обязательств; отгрузку, передачу, поставку, перемещения товаров
- Контракт (договор) и иные документы, являющиеся основанием для проведения валютных операций
- Ведомость банковского контроля
- Письма, заявления, справочная информация и иные документы, оформление которых может быть предусмотрено иными договорами, заключенными между Клиентом и Банком, предусматривающие использование Системы ДБО
- Файлы зарплатных проектов

При этом остальные непоименованные выше документы свободного формата носят исключительно информационный характер, если иное не предусмотрено дополнительными договоренностями между Сторонами, содержащими ссылку на Соглашение.

7.7 ЭД должны содержать все необходимые реквизиты согласно требованиям Банка, Банка России, а также описанию используемой подсистемы Системы ДБО.

7.8 ЭД, поступившие от Клиента, не подлежат редактированию сотрудниками Банка.

7.9 ЭД порождает обязательства Сторон, если он надлежащим образом оформлен Клиентом, заверен необходимым количеством зарегистрированных ЭП Клиента в соответствии с их назначением, передан по Системе ДБО и прошел в Банке процедуры приема к исполнению. Свидетельством того, что ЭД принят к исполнению, является изменение статуса ЭД в Системе ДБО, о чем Банк размещает в Системе ДБО электронное извещение.

7.10 Претензии по поводу исполнения/неисполнения ЭД не могут быть заявлены ни одной из Сторон по истечении 10 (десяти) дней с момента получения Клиентом выписки по Счету с использованием Системы ДБО или на бумажном носителе. В случае если Клиент не заявит претензии к Банку в течение установленного срока, выписка по Счету считается подтвержденной.

7.11 Банк уведомляет Клиента обо всех расчетных операциях, совершенных с использованием Системы ДБО, в соответствии со следующим порядком:

7.11.1 Уведомление Клиента о приеме ЭПД, а также о совершении операции на основании принятого ЭПД осуществляется в режиме реального времени.

7.11.2 Уведомление о совершении расчетной операции осуществляется путем направления Клиенту электронного квитка, присоединяемого к исполненному ЭПД и отражающего статус ЭПД «исполнено» (далее – электронный квиток). Электронный квиток и ЭПД, к которому он присоединен, составляют единое целое и являются Извещением, подтверждающим осуществление расчетной операции с использованием Системы ДБО.

7.11.3 Выписка по Счету предоставляется Банком на основании полученного от Клиента ЭД «Запрос выписки». Полная информация о движениях по Счету за операционный день предоставляется в выписке, подготовленной после завершения данного операционного дня. Отсутствие движений по Счету за операционный день подтверждается наличием не содержащей движений по Счету выписки, подготовленной после завершения данного операционного дня.

7.11.4 Функционал визирования документов предоставляется Клиентам только после надлежащего дополнительного юридического оформления (трехстороннее соглашение между Банком, Клиентом и визирующей организацией).

7.11.5 Сообщения о расчетных операциях доводятся до сведения Клиента при иницировании последним сеанса связи с Банком.

7.11.6 Банк фиксирует в Системе ДБО факт направления Клиенту Сообщений о расчетных операциях и хранит их электронные копии не менее 3 (трех) лет.

8. Права и обязанности Сторон

Стороны обязуются при проведении расчетных операций (либо при осуществлении электронного документооборота) с использованием Системы ДБО руководствоваться правилами и требованиями, установленными Центральным банком Российской Федерации, законодательством Российской Федерации, Правилами и приложениями к ним.

8.1. Взаимные права и обязанности Сторон

8.1.1. Каждая сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для проведения электронных расчетов по Системе ДБО в соответствии с Правилами.

8.1.2. Стороны обязуются не разглашать третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации или дополнительным соглашением Сторон, конкретные способы защиты информации, реализованные в используемой по Правилам Системе ДБО, а также иные условия Соглашения, известные только Сторонам.

8.1.3. Стороны обязуются сохранять в тайне от третьих лиц применяемые в Системе ДБО защиты информации закрытые ключи и периодически, не реже одного раза в 15 (пятнадцать) месяцев, проводить их плановую замену. Плановой заменой ключей считается замена ключа Уполномоченного лица без изменения режима подписи, производимая не ранее 12 (двенадцати) месяцев с даты изготовления ключа.

8.1.4. Каждая из Сторон обязуется немедленно информировать другую сторону обо всех случаях компрометации закрытых ключей или о подозрении в их компрометации, в том числе, о случаях утраты, хищения, несанкционированного использования ключей, а также повреждения программно-технических средств подсистем обработки, хранения, защиты и передачи информации для своевременного проведения внеплановой смены ключей и других согласованных действий по поддержанию в рабочем состоянии Системы ДБО. При этом работа по Системе ДБО приостанавливается до проведения внеплановой смены скомпрометированных ключей и устранения повреждений Системы ДБО.

8.2. Права и обязанности Клиента

8.2.1. Клиент обязуется произвести все действия, необходимые для введения в эксплуатацию программного обеспечения, переданного Клиенту Банком, и подписать Акт о начале использования Системы ДБО в течение 10 (десяти) рабочих дней с момента передачи Банком Клиенту программного обеспечения.

8.2.2. Клиент по завершении подготовительных процедур непосредственно перед началом использования Системы ДБО подписывает двухсторонний Акт о начале использования Системы ДБО по форме Приложения № 6 к Правилам.

8.2.3. Клиент обязуется обеспечивать сохранность и защиту от использования не по назначению закрытых ключей ЭП.

8.2.4. Клиент обязан до истечения 15 (пятнадцати) месяцев с момента выдачи Банком Карточек регистрации произвести необходимые действия, направленные на смену ключей, соответствующих выданным Карточкам регистрации, и представить в Банк по 3 (три) экземпляра Акта признания каждого Ключа проверки электронной подписи, оформленного по форме Приложения № 5 к Правилам.

8.2.5. Клиент несет ответственность за использование криптографических ключей Клиента и обязуется самостоятельно обеспечить доступность, целостность и конфиденциальность ключей Клиента.

8.2.6. Клиент имеет право направить отзыв своего распоряжения с помощью Системы ДБО. Отзыв распоряжения осуществляется до наступления безотзывности исполнения. Банк принимает к исполнению отзыв ЭД только в том случае, если у Банка имеется технологическая возможность отменить его исполнение. Заявление об отзыве служит основанием для возврата (аннулирования) Банком распоряжения Клиента.

8.2.7. Стороны устанавливают, что вся информация по Системе ДБО считается доведенной до сведения Клиента по истечении 3 (трех) банковских дней с даты ее размещения Банком в Системе ДБО, включая день размещения.

8.2.8. По письменному требованию Банка Клиент в течение 3 (трех) рабочих дней с момента получения указанного письменного требования обязан передать Банку курьером или заказным письмом копии ЭД, переданных по Системе ДБО и проведенных Банком в течение периода, указанного в письменном требовании Банка, на бумажном носителе. Копии документов должны быть оформлены Клиентом в соответствии с законодательством Российской Федерации и заверены собственноручными подписями руководителя, главного бухгалтера (при наличии) и печатью Клиента. Содержание бумажных копий должно полностью совпадать с содержанием соответствующих ЭД.

8.2.9. Клиент обязуется установить и использовать при проведении электронных расчетов переданное Банком программное обеспечение Системы ДБО только на исправном и проверенном на отсутствие вредоносного программного обеспечения оборудовании, соблюдать порядок Безопасного использования дистанционного банковского обслуживания, содержащийся в п. 4 Приложения № 1 к Правилам. Проверки оборудования на предмет наличия вредоносного программного обеспечения должны проводиться Клиентом ежедневно.

8.2.10. Клиент обязуется оплачивать комиссии Банку за установку и обслуживание Системы ДБО, иных оказанных Клиенту услуг в процессе использования Системы ДБО.

8.2.11. В случае утраты электронного средства платежа и (или) его использования без согласия Клиента, в том числе при компрометации Ключа электронной подписи, Клиент обязан в соответствии с Приложением № 1 к Правилам направить в Банк уведомление в форме Заявления о компрометации ключей системы защиты информации по форме Приложения № 7 к Правилам или Заявления об использовании ключей защиты информации без согласия Клиента по форме Приложения № 9 к Правилам незамедлительно после обнаружения соответствующего факта, но не позднее дня, следующего за днем получения от Банка уведомления о совершенной операции.

8.2.12. Клиент обязан ежедневно осуществлять вход в Систему ДБО в целях своевременного получения информации и сообщений от Банка.

8.2.13. Клиент имеет право в любое время провести процедуру смены ключей ЭП в порядке, предусмотренном Приложением № 1 к Правилам.

8.2.14. Клиент не имеет права тиражировать, декомпилировать и передавать третьей стороне программное обеспечение, предоставляемое Банком.

8.2.15. При расторжении Соглашения Клиент обязуется уничтожить всё переданное ему в соответствии с Соглашением программное обеспечение.

8.3. Права и обязанности Банка

8.3.1. Банк обязуется передать Клиенту программное обеспечение, реквизиты доступа Клиента к Системе ДБО в течение 5 (пяти) рабочих дней с момента заключения Соглашения.

Банк производит подключение Клиента к Системе ДБО, а также установку и настройку программного обеспечения Системы ДБО на технических средствах Клиента, если Клиент запросил предоставление данной услуги.

8.3.2. Банк обязан в случае необходимости консультировать Клиента по вопросам установки и работы Системы ДБО в процессе эксплуатации указанной системы.

8.3.3. Банк обязуется обеспечить надлежащее хранение Карточек регистрации и эталонного образца программного обеспечения.

8.3.4. Банк обязуется уведомлять Клиента обо всех операциях, совершенных с использованием Системы ДБО в порядке, установленном п.7.11. Правил.

8.3.5. Банк обязуется фиксировать направленные Клиенту и полученные от Клиента уведомления, а также хранить соответствующую информацию не менее 5 (пяти) лет.

8.3.6. Банк обязуется предоставлять Клиенту информацию, связанную с использованием Системы ДБО и электронного средства платежа.

8.3.7. Банк вправе по истечении 15 (пятнадцати) месяцев с момента выдачи Банком Карточек регистрации приостановить использование соответствующих ключей Клиента в случае, если Клиент не произвел необходимые действия, направленные на смену ключей, соответствующих выданным Карточкам регистрации, и не представил в Банк по 3 (три) экземпляра надлежаще оформленных Актов признания каждого Ключа проверки электронной подписи.

8.3.8. Банк обязуется осуществлять перевод денежных средств Клиента на основании ЭПД Клиента, поступивших по Системе ДБО, в порядке, предусмотренном законодательством, в том числе нормативными актами Банка России, а также соответствующими Договорами банковского счета / иными договорами, заключенными между сторонами.

8.3.9. Банк вправе запрашивать по отдельным ЭД дополнительные разъяснения и подтверждения. Подтверждения запрашиваются не позднее рабочего дня, следующего за днем получения ЭД по Системе ДБО либо иным способом. В таком случае полученный Банком ЭД исполняется после получения Банком необходимых подтверждений.

8.3.10. Банк вправе отказать Клиенту в исполнении принятого от него ЭПД, кроме случаев, указанных в Правилах, в случае признания Банком операций Клиента сомнительными и/или совершаемыми в целях легализации доходов или финансирования терроризма, а также в иных случаях, предусмотренных законодательством Российской Федерации и внутренними нормативными актами Банка о противодействии легализации доходов и финансированию терроризма.

8.3.11. Банк вправе отказать Клиенту в предоставлении услуг по Соглашению в части использования Системы ДБО для исполнения ЭПД Клиента, в случаях обнаружения Банком Счетов Клиента, которые не используются Клиентом либо использование которых подпадает под признаки, указанные в рекомендациях Банка России, данных в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Банк также вправе возобновить оказание услуг по Соглашению в части использования Системы ДБО для исполнения ЭПД Клиента.

8.3.12. Банк отказывает Клиенту в предоставлении услуг по Соглашению в части использования Системы ДБО для исполнения ЭПД Клиента, незамедлительно, но не позднее одного рабочего дня: - со дня размещения в сети Интернет на официальном сайте Федеральной службы по финансовому мониторингу (далее - Уполномоченный орган) информации о включении Клиента в перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму, либо - со дня размещения в сети Интернет на официальном сайте Уполномоченного органа решения о применении мер по замораживанию (блокированию) денежных средств или иного имущества, принадлежащего Клиенту, в отношении которого имеются достаточные основания подозревать его причастность к террористической деятельности (в том числе к финансированию терроризма) при отсутствии оснований для включения в указанный перечень Клиента, и в отношении которого Межведомственной комиссией по противодействию финансированию терроризма приняты решения о замораживании (блокировании) принадлежащих таким Клиентам денежных средств или иного имущества. Банк возобновляет оказание услуг по Соглашению в части использования Системы ДБО для исполнения ЭПД Клиента не позднее одного рабочего дня со дня размещения в сети Интернет на официальном сайте Уполномоченного органа оснований для отмены решения о включении Клиента в перечень организаций и физических лиц, в отношении которого имеются сведения об их причастности к экстремистской деятельности или терроризму, или со дня получения Банком информации об основаниях для отмены решений о применении мер по замораживанию (блокированию) денежных средств или иного имущества.

8.3.13. Банк вправе приостановить предоставление Клиенту услуг по Соглашению в части использования Системы ДБО в случае обнаружения повторяющихся попыток получения доступа к Системе ДБО от имени Клиента с нарушениями условий безопасного доступа Клиента.

8.3.14. Банк обязан по требованию Клиента предоставлять на бумажном носителе выписки по Счету (для Клиентов, которым открыт Счет в Банке), а также по запросу Клиента предоставлять копии ЭД на бумажном носителе с отметкой о принятии к исполнению.

8.3.15. Банк имеет право оформлять бумажные копии принятых к исполнению ЭПД Клиента и заверять их.

8.3.16. Банк обязуется обеспечить конфиденциальность информации о расчетных операциях по Счету, проводимых в соответствии с Соглашением, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.3.17. Банк оставляет за собой право отключения Клиента от Системы ДБО в случае нарушений со стороны Клиента условий Соглашения.

9. Ответственность Сторон

9.1. За неисполнение или ненадлежащее исполнение обязательств по Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

9.2. Банк не несет ответственности за сбои в обмене ЭД, возникшие в результате наличия на технических средствах Клиента вредоносного программного обеспечения (вирусов), неисправности каналов связи, сбоев в работе провайдеров телекоммуникационных услуг, отключения или перебоев в линиях электропитания, неисправности технических средств Клиента.

9.3. Стороны не несут ответственности за задержки, сбои и другие недостатки в исполнении обязательств по Правилам в случае возникновения обстоятельств непреодолимой силы, которые Стороны не могли предвидеть и предотвратить своими силами (форс-мажор), включая, но не ограничиваясь стихийными бедствиями, военными действиями, забастовками, изданием актов государственной власти Российской Федерации (законодательной, исполнительной, судебной).

9.4. В случае нарушения условий Правил и приложений к ним ответственность за последствия несет Сторона, которая допустила эти нарушения.

9.5. Клиент не может требовать от Банка возмещения убытков, возникших в результате:

- перевода неуполномоченным лицом средств из-за нарушения Клиентом условий Правил и приложений к ним, в том числе ненадлежащего хранения и использования закрытых ключей ЭП, которое могло повлечь возможность неправомерного использования закрытых ключей ЭП третьими лицами;
- перевода неуполномоченным лицом средств вследствие компрометации криптографических ключей Клиента, произошедшей из-за присутствия вредоносного программного обеспечения на оборудовании, используемом Клиентом при проведении электронных расчетов в Системе ДБО;
- перевода неуполномоченным лицом средств в случае если Банк исполняет обязанность по уведомлению Клиента о расчетных операциях, совершенных с использованием Системы ДБО в порядке, установленном п. 7.11. Правил, и не получил от Клиента уведомление в форме Заявления о компрометации соответствующих ключей системы защиты информации в соответствии с п. 8.2.12. Правил до осуществления несанкционированного перевода;
- неправильного оформления Клиентом ЭД.

9.6. Банк не несет ответственности за убытки, понесенные Клиентом не по вине Банка в результате использования Системы ДБО, в том числе при исполнении ошибочных ЭПД, если эти документы надлежащим образом Клиентом оформлены и переданы, а Банком получены, проверены и приняты в соответствии с порядком, установленным Правилами.

9.7. Банк не несет ответственности в случае если при исполнении Сторонами Соглашения конфиденциальная информация об электронных расчетах Клиента станет известна третьим лицам не по вине Банка.

10. Финансовые взаимоотношения

10.1. Банк безвозмездно предоставляет Клиенту во временное пользование на весь срок действия Соглашения:

- программное обеспечение Системы ДБО;
- один экземпляр программного обеспечения средства криптографической защиты информации.

При этом в случае возникновения у Клиента необходимости вывоза с территории Российской Федерации указанного программного обеспечения средства криптографической защиты информации, данный вопрос решается Клиентом самостоятельно, без какого-либо участия Банка.

10.2. Банк бесплатно предоставляет Клиенту электронную документацию по Системе ДБО.

10.3. Предоставляемые Клиенту дистрибутивы и документация доступны на официальном сайте Банка по адресу: <http://www.bank-peresvet.ru/dbo/>.

10.4. Всё оборудование и прочее программное обеспечение согласно Приложению № 2 к Правилам Клиент приобретает самостоятельно за собственный счет у третьих лиц.

10.5. Датой оказания услуг по подключению Клиента к Системе ДБО, изготовлению Карточек регистрации считается дата размещения изготовленных Банком соответствующих Карточек регистрации в Системе ДБО.

10.6. Услуги по установке программного обеспечения на технические средства Клиента, а также иные услуги, оказываемые Банком Клиенту в рамках Соглашения, предоставляются при условии предварительной оплаты (для Клиентов, которым Счет в Банке не открыт) или наличия достаточных средств для оплаты комиссий Банку на Счете Клиента (для Клиентов, которым открыт Счет в Банке).

10.7. В случае наличия задолженности Клиента по оплате комиссий Банка, связанных с установкой и обслуживанием Системы ДБО, более 10 (десяти) календарных дней Банк вправе в одностороннем порядке приостановить обслуживание Счета Клиента и/или обслуживания Клиентов в рамках заключенного Договора банковского счета / иного договора в Системе ДБО. Повторное подключение Клиента осуществляется на основании письменного заявления, при условии полного погашения всей имеющейся задолженности по комиссиям перед Банком. За повторное подключение Банком взимается комиссионное вознаграждение в размере, установленном действующими Тарифами Банка.

11. Срок действия Соглашения

11.1. Соглашение вступает в силу в части обязательств по подключению Клиента к Системе ДБО с момента заключения Соглашения (п.4.2.4. Правил), в остальной части – с момента подписания Акта о начале использования Системы ДБО, и действует до даты прекращения действия всех Договоров банковского счета / иных договоров, на которые распространяется действие Соглашения, или до даты расторжения Соглашения.

11.2. Соглашение в полном объеме вступает в силу с даты подписания Акта о начале использования Системы ДБО. В случае не подписания Клиентом Акта о начале использования Системы ДБО в течение 3 (трех) календарных месяцев со дня заключения Соглашения, настоящее Соглашение может быть расторгнуто Банком в одностороннем порядке.

11.3. В случае отсутствия ЭПД от Клиента в течение 3 (трех) календарных месяцев настоящее Соглашение может быть расторгнуто Банком в одностороннем порядке. Повторное подключение Клиента к Системе ДБО в таком случае производится путем заключения нового Соглашения.

11.4. Соглашение может быть расторгнуто по письменному заявлению Клиента с предупреждением об этом Банка не менее чем за 15 (пятнадцать) календарных дней.

11.5. В случае неисполнения или ненадлежащего исполнения Клиентом условий Соглашения Банк имеет право расторгнуть Соглашение в одностороннем порядке с предупреждением об этом Клиента не менее чем за 2 (два) рабочих дня.

11.6. В случае неисполнения или ненадлежащего исполнения Банком условий Соглашения Клиент имеет право расторгнуть Соглашение в одностороннем порядке с предупреждением об этом Банка не менее чем за 2 (два) рабочих дня.

11.7. Стороны согласны с тем, что в части неразглашения паролей и ключей системы защиты информации Соглашение остается в силе в течение 1 (одного) календарного года с момента его расторжения.

11.8. Уведомление об отказе от Соглашения должно быть направлено по почте заказным письмом или передано лично.

12. Изменение и дополнение Правил

12.1. Внесение изменений и дополнений в Правила и приложения производится Банком в одностороннем порядке путем утверждения новой редакции Правил.

12.2. Изменения и дополнения, вносимые Банком в Правила в связи с изменением законодательного и нормативного регулирования, вступают в силу одновременно с вступлением в силу изменений в указанные акты.

12.3. Банк уведомляет Клиентов о вступлении в силу изменений и дополнений в Правила, вносимых Банком по собственной инициативе и не связанных с изменением законодательства Российской Федерации, нормативных актов Банка России, не менее чем за 10 (десять) календарных дней до вступления в силу изменений или дополнений. Все изменения и дополнения, вносимые Банком в настоящие Правила по собственной инициативе, вступают в силу через 10 (десять) календарных дней после уведомления Клиента путем публикации изменений и дополнений на официальном сайте Банка в информационно-телекоммуникационной сети Интернет.

12.4. Клиент обязуется с целью своевременного ознакомления с изменениями и дополнениями Правил каждые 5 (пять) дней посещать официальный сайт Банка в сети Интернет.

12.5. Изменения и дополнения в Правилах с момента вступления их в силу в порядке, установленном настоящим разделом Правил, распространяются на всех Клиентов, включая тех Клиентов, которые заключили Соглашение ранее даты вступления изменений и дополнений Правил в силу. В случае несогласия с изменениями или дополнениями, внесенными в Правила и/или приложения к ним Банком, Клиент вправе расторгнуть Соглашение в порядке, установленном Правилами не позднее 7 (семи) рабочих дней с даты введения новых редакций Правил.

12.6. Стороны вправе дополнить свои права и обязанности, предусмотренные Соглашением и изложенные в Правилах, путем заключения дополнительного соглашения к Соглашению.

13. Урегулирование претензий и рассмотрение споров Сторон

13.1. Претензии и споры, возникающие при исполнении Правил, рассматриваются и решаются в порядке, установленном Договорами банковского счета / иными договорами, за исключением споров и конфликтных ситуаций по поводу подлинности ЭД и использования Клиентом электронного средства платежа (проведение расчетных операций, совершенных с использованием Системы ДБО без согласия Клиента).

13.2. В случае возникновения между Сторонами разногласий относительно подлинности ЭД и использования Клиентом электронного средства платежа (проведение расчетных операций, совершенных с использованием Системы ДБО, без согласия Клиента), такие разногласия разрешаются в соответствии с Приложением № 1 к Правилам.

14. Обработка персональных данных

14.1. Обработка персональных данных Уполномоченных лиц, предоставленных Клиентом в Банк согласно Правилам, осуществляется в целях исполнения настоящего Соглашения в соответствии с ч. 2 ст. 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

Перечень действий с персональными данными, общее описание способов обработки персональных данных: любые действия (операции) или совокупность действий (операций), включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных, как с использованием средств автоматизации, так и без использования таких средств.

Срок обработки персональных данных: с момента предоставления в Банк до истечения 5 (пяти) лет после прекращения настоящего Соглашения.

15. Заключительные положения

15.1. Неотъемлемой частью настоящего Соглашения являются:

- Приложение № 1. Порядок организации электронных расчетов посредством Системы дистанционного банковского обслуживания BS-Client v.3
- Приложение № 2. Требования подсистем ДБО к программным, техническим средствам, каналам связи
- Приложение № 3. Заявление на конфигурирование АРМ Системы ДБО BS-Client v.3
- Приложение № 4. Акт приема-передачи
- Приложение № 5. Акт признания ключа проверки электронной подписи
- Приложение № 6. Акт о начале использования Системы ДБО
- Приложение № 7. Заявление о компрометации ключей системы защиты информации
- Приложение № 8. Форма доверенности
- Приложение № 9. Заявление об использовании ключей защиты информации без согласия Клиента

Приложение № 1
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

**Порядок организации электронных расчетов посредством
Системы дистанционного банковского обслуживания BS-Client v.3**

1. Основные используемые понятия:

- 1.1. **Акт признания ключа проверки электронной подписи (Акт признания ключа)** – документ, содержащий распечатку ключа проверки электронной подписи Клиента в шестнадцатеричной системе счисления, сведения о Клиенте – юридическом лице, сведения об Уполномоченном лице Клиента, обладающем правом использования ЭП, подписанный Клиентом и заверенный оттиском печати Клиента (Приложение № 3 к Правилам).
- 1.2. **Зарегистрированный ключ** - ключ проверки электронной подписи, размещенный в каталоге ключей, ключ проверки электронной подписи ЦУКС Банка.
- 1.3. **Зарегистрированный Клиент** - пользователь Системы ДБО, ключи проверки электронной подписи Уполномоченных лиц которого размещены в каталоге ключей проверки электронной подписи ЦУКС Банка.
- 1.4. **Запрос на выдачу Карточки регистрации Ключа проверки электронной подписи Уполномоченного лица Клиента (запрос на выдачу Карточки регистрации)** – электронный документ, подписанный действующим ключом ЭП Уполномоченного лица, который включает в себя новый ключ проверки электронной подписи Клиента. Запрос на выдачу Карточки регистрации создается средствами ЭП автоматически в процессе генерации новой пары ключей ЭП Уполномоченного лица.
- 1.5. **Интернет Клиент-Банк** – подсистема Системы ДБО. Подключение данной подсистемы позволяет организовать дистанционное банковское обслуживание наиболее простым способом с возможностью использования на мобильном или стационарном компьютере.
- 1.6. **Каталог ключей проверки электронной подписи** - совокупность действующих ключей проверки электронной подписи, наименований Клиентов и иной служебной информации.
- 1.7. **Плановая смена ключа ЭП** – процедура замены криптографического ключа Уполномоченного лица, проводимая по инициативе Клиента по истечении 12 (двенадцати) месяцев с момента выпуска соответствующей Карточки регистрации, не связанная с компрометацией ключа.
- 1.8. **Центр управления ключевыми системами (ЦУКС) Банка** – организационная структура Банка, выполняющая функции регистрации и ведения базы ключей проверки электронной подписи Клиентов.

2. Общие положения.

- 2.1. Настоящий документ устанавливает порядок организации и проведения обмена электронными документами, в частности электронных расчетов, между Банком и Клиентом.
- 2.2. Абонентский пункт Клиента состоит из персонального компьютера, общесистемного программного обеспечения и программного обеспечения Системы ДБО в составе и в соответствии с требованиями, указанными в Приложении № 2 к Соглашению.
- 2.3. Абонентский пункт Банка принимает документы, передаваемые Клиентом по Системе ДБО, а также размещает всю необходимую информацию для Клиента в Системе ДБО в автоматическом режиме.
- 2.4. Для обслуживания Системы ДБО Банк организует работу службы поддержки клиентов, в обязанности которой входит:
 - обеспечение бесперебойной работы Системы ДБО;
 - помощь при установке и настройке Клиентом программного обеспечения Системы ДБО;
 - консультационная поддержка персонала Клиента;
 - поддержка ключевого управления в Системе ДБО.

3. Процедуры создания, обновления, регистрации и действия при компрометации ключей криптографической защиты.

- 3.1. Процедуры регистрации и проверки ключей системы защиты информации происходят на базе ЦУКС Банка по адресу: 123100, Москва, Краснопресненская наб., д. 14.
- 3.2. Акты признания ключей оформляются отдельно на каждый ключ ЭП.
- 3.3. Дата и время ввода ключа в действие совпадает с датой и временем изготовления Банком соответствующей Карточки регистрации. Дата и время вывода ключей из действия определяется моментом вывода ключей Банком из действия в соответствии с Заявлениями Клиента, моментом завершения срока действия Карточки регистрации, либо датой и временем расторжения Соглашения. Вывод ключа из действия осуществляется:
- в случае изменения режима подписи Уполномоченного лица вывод из действия ключа со старым режимом подписи производится при обработке Заявления Клиента в ЦУКС Банка. Вывод из действия ключа со старым режимом подписи производится не позднее 18:00 в день размещения Карточки регистрации Уполномоченного лица с новым режимом подписи в Системе ДБО. После вывода ключа из действия все ЭПД, подписанные данным ключом, отбраковываются Системой ДБО;
 - в случае плановой либо досрочной смены ключа Уполномоченного лица, а также в случае замены одного Уполномоченного лица другим вывод из действия старого ключа производится после успешного завершения Клиентом процедуры приема Карточки регистрации нового Ключа проверки электронной подписи. Банк выводит из действия старый ключ не позднее 18:00 московского времени рабочего дня, следующего за днём приёма Клиентом Карточки регистрации нового Ключа проверки электронной подписи;
 - в случае отзыва прав Уполномоченного лица вывод из действия ключа производится не позднее рабочего дня, следующего за днём поступления Заявления Клиента в Банк. Использование выведенного из действия ключа в Системе ДБО невозможно.
- 3.4. При необходимости экстренного отзыва прав Уполномоченного лица Клиент оформляет Заявление о компрометации ключей системы защиты информации по форме Приложения № 7 к Соглашению. В указанном случае вывод ключа из действия осуществляется в максимально сжатые сроки.

Этапы работы	Исполнитель
Подключение Клиента. Выбор услуг ДБО.	
1. Подписание и передача в Банк Заявления на конфигурирование АРМ Системы ДБО.	Клиент
2. Предоставление документов на Уполномоченных лиц.	
3. Изготовление копии Заявления Клиента, регистрация Заявления, предоставление Клиенту копии заявления с регистрационной информацией.	Банк
4. Заведение Клиента в системе ДБО, подготовка установочного комплекта для передачи Клиенту не позднее 5 рабочих дней с момента поступления Заявления в Банк.	
5. Передача Клиенту установочного комплекта, согласно выбранному в Заявлении способом. Установочный комплект передается в соответствии с Приложением №4.	
6. Установка необходимого для работы ПО. Перечень необходимого ПО и оборудования указан в Приложении № 2 данных правил.	
7. Предоставление в Банк 2 (двух) экземпляров Акта приема-передачи, подписанного со стороны Клиента.	
8. Генерация пары рабочих ключей ЭП (Ключа электронной подписи и Ключа проверки электронной подписи), формирование запроса на выдачу Карточки регистрации, передача запроса на выдачу Карточки регистрации в Банк по Системе ДБО.	Клиент
9. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого ключа. Передача 3 (трех) экземпляров Акта в Банк. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента.	
10. Печать, заполнение и подписание 2 (двух) экземпляров Акта о начале использования Системы ДБО.	
11. Передача в Банк Актов признания каждого ключа и Актов о начале использования Системы ДБО.	
12. Сравнение Акта признания и запроса на выдачу Карточки регистрации. При	
	Банк

<p>положительном результате сравнения производится выдача Карточек регистрации и брелоков для генерации одноразовых паролей.</p> <p>13. Подключение указанного Клиентом способа защиты Клиент-Банка, согласно п. 5 Заявления. Размещение Карточки регистрации в Системе ДБО для получения Клиентом. С данного момента Клиент считается Зарегистрированным и функционал системы ДБО доступен ему в полном объеме.</p> <p>14. Подписание Актов приема-передачи со стороны Банка.</p> <p>15. Подписание Акта о начале использования со стороны Банка.</p>	
Плановая смена рабочих ключей Клиента в процессе использования Системы ДБО.	
<p>1. Генерация пары (ключ электронной подписи и ключ проверки электронной подписи) новых ключей ЭП, формирование запроса на выдачу Карточки регистрации, передача подписанного на действующем ключе ЭП запроса на выдачу Карточки регистрации в Банк по Системе ДБО. Предоставления Заявления на конфигурирование Системы ДБО не требуется.</p> <p>2. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого ключа. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента.</p> <p>3. Передача документов в Банк.</p>	Клиент
<p>4. Сравнение Акта признания и запроса* на выдачу Карточки регистрации. При положительном результате сравнения выдача Карточки регистрации. Размещение Карточки регистрации в Системе ДБО для получения Клиентом.</p> <p><i>* Запрос Клиента на выдачу Карточки регистрации хранится в Банке в течение 180 (ста восьмидесяти) дней, после чего аннулируется.</i></p>	Банк
Внеплановая смена рабочих ключей Клиента в процессе использования Системы ДБО.	
<p>1. Подписание и передача в Банк Заявления на конфигурирование АРМ Системы ДБО. Заявление должно содержать требование одновременного внесения следующих изменений перечня Уполномоченных лиц, режимов подписи:</p> <ul style="list-style-type: none"> • вывести из действия (отключить) используемые ключи; • изготовить новые (подключить) профили. <p>2. После передачи в Банк Заявления на конфигурирование АРМ Системы ДБО необходимо действовать в порядке:</p> <ul style="list-style-type: none"> • установленном для начального подключения, в случае заказа восстановления начальных настроек; • установленном для плановой смены рабочих ключей Клиента в процессе использования Системы ДБО, в остальных случаях. 	Клиент
Компрометация ключа Уполномоченного лица Клиента.	
<p>1. Клиент оформляет Заявление о компрометации ключей системы защиты информации и передает в Банк по факсу, электронной почте или нарочным в офис Банка.</p>	Клиент
<p>2. Банк производит временное блокирование ключей Клиента.</p>	Банк
<p>3. Клиент передаёт оригинал Заявления о компрометации ключей системы защиты информации в Банк.</p>	Клиент
<p>4. В случае если оригинал Заявления компрометации ключей не поступил в Банк до окончания рабочего дня, следующего за днём временного блокирования ключей, работа в Системе ДБО с использованием временно заблокированных ключей возобновляется.</p> <p>5. При поступлении в Банк оригинала Заявления о компрометации ключей системы защиты информации Банк фиксирует факт компрометации ключей Клиента и блокирует дальнейшее использование скомпрометированных ключей. Дальнейшее использование скомпрометированного ключа возможно только в качестве технологического.</p>	Банк
<p>6. Клиент проводит обновление ключей, зарегистрированных в ЦУКС Банка, в порядке, установленном для внеплановой смены ключа.</p>	Клиент

Добавление Уполномоченного лица, изменение режима подписи.	
1. Оформление и передача в Банк 1 (одного) экземпляра Заявления на конфигурирование АРМ Системы ДБО и необходимых документов на Уполномоченные лица.	Клиент
2. Генерация Профиля Ключа Клиента для каждого Уполномоченного лица.	Банк
3. Генерация пары (ключ электронной подписи и ключ проверки электронной подписи) рабочих ключей ЭП, формирование запроса на выдачу Карточки регистрации, передача запроса на выдачу Карточки регистрации в Банк по Системе ДБО.	Клиент
4. Печать, заполнение и подписание 3 (трех) экземпляров Акта признания каждого ключа. Акт признания ключа подписывается Уполномоченным лицом, руководителем Клиента и заверяется оттиском печати Клиента.	
5. Передача 3 (трех) экземпляров Акта признания ключа в Банк.	
6. Проверка Акта признания, Заявления на внесение изменений в Систему ДБО и запроса на выдачу Карточки регистрации. При положительном результате проверки производится выдача Карточки регистрации.	Банк
7. Размещение Карточки регистрации в Системе ДБО для получения Клиентом. С данного момента ключ Клиента считается Зарегистрированным и функционал системы ДБО доступен ему в полном объеме.	
Расторжение Соглашения.	
1. Исключение ключей Клиента из каталога ключей ключа проверки электронной подписи Банка.	Банк
2. Блокирование работы Клиента в Системе ДБО.	

4. **Безопасное использование систем дистанционного банковского обслуживания.**

- 4.1. Клиент должен самостоятельно генерировать криптографические ключи.
- 4.2. Закрытые криптографические ключи должны храниться на съемных носителях информации в недоступном неуполномоченным лицам месте. Ключевые носители должны извлекаться из хранилища только на время непосредственного использования. Ключевые носители не должны быть доступны для посторонних лиц от момента генерации до момента уничтожения ключей. Ответственность за организацию надлежащего хранения закрытых ключей Клиента несет Клиент.
- 4.3. Для резервных копий ключевых носителей необходимо соблюдение тех же правил обращения с ними, которые установлены для основных носителей.
- 4.4. После выведения закрытых криптографических ключей из действия такие ключи должны уничтожаться.
- 4.5. При возникновении подозрения на компрометацию пароля входа в Систему ДБО или криптографических ключей такой пароль или ключи должны быть немедленно заменены. Криптографические ключи должны меняться ежегодно в плановом порядке.
- 4.6. Использование для работы в Системе ДБО гостевых рабочих мест (интернет-кафе и т.п.) не рекомендуется по причине повышенного риска кражи криптографических ключей и паролей доступа.
- 4.7. При невозможности установления связи с серверами ДБО Банка Клиенту следует обратиться в Единый Центр сопровождения ДБО Банка.
- 4.8. Необходимо строго соблюдать требования по организационному обеспечению эксплуатации СКЗИ, требования по размещению СКЗИ и режиму охраны, требования по обеспечению безопасности ключевой информации, содержащиеся в документации на СКЗИ.
- 4.9. Необходимо обеспечить защиту от рисков, связанных с распространением вредоносного программного обеспечения. Меры по защите рабочего места Системы ДБО должны включать:
 - использование только лицензионного программного обеспечения, получаемого из надежных источников;
 - своевременную установку обновлений безопасности используемого программного обеспечения (операционная система, веб браузер, офисное программное обеспечение и т.п.);
 - использование только необходимого для работы программного обеспечения;
 - использование регулярно обновляемого антивирусного программного обеспечения;

- использование средств сетевой защиты (межсетевого экрана) и средств обнаружения вторжений (IDS/IPS);
 - ограничение использования публичных сетей, файлового обмена и сообщений электронной почты;
 - контроль целостности исполняемых файлов и файлов конфигураций;
 - использование многофакторной авторизации, согласованных с Банком идентификационных признаков компьютера Клиента (фильтрация по MAC и внешним IP-адресам, одноразовых паролей на брелоках eToken PASS) и иных дополнительных средств обеспечения безопасности, предоставляемых Банком;
 - проведение плановой регенерации ключей ЭП не реже одного раза в 15 (пятнадцать) месяцев;
 - установку пароля на контейнер ЭП в СКЗИ;
 - своевременное обновление клиентского программного обеспечения системы ДБО до рекомендованной Банком в информационных письмах версии;
 - использование безопасного входа в подсистему «Интернет-Клиент» ДБО через виртуальную клавиатуру;
 - осуществление смены пароля Клиента на вход в Систему ДБО и контейнер СКЗИ не реже 1 (одного) раза в квартал;
 - недопущение установки ранее использованных, коротких и простых (менее 3 (трех) групп символов) паролей;
 - незамедлительное информирование Банка о хищении или компрометации средств идентификации, ключей ЭП Клиента в Системе ДБО;
 - другие меры, признанные целесообразными.
- 4.10. Необходимо обеспечить защиту от несанкционированного доступа к оборудованию и программному обеспечению СКЗИ третьих лиц.
- 4.11. Размещение, специальное оборудование, охрана и организация режима в помещениях, в которых установлены СКЗИ или хранятся криптографические ключи, должны обеспечивать сохранность СКЗИ и криптографических ключей. Такие помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие (для юридических лиц - в том числе в нерабочее время). Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в такие помещения посторонних лиц, необходимо оборудовать металлическими решетками или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению.
- 5. Порядок передачи и приема документов по Системе ДБО.**
- 5.1. Инициатором проведения всех расчетных операций, получения информации по Системе ДБО, смены ключей Клиента является Клиент, для чего он формирует соответствующие запросы, в ответ на которые Банк предоставляет затребованную либо принимает переданную информацию.
- 5.2. Информация, размещенная Банком в Системе ДБО, становится доступной для Клиента с момента размещения при условии установления Клиентом авторизованного сеанса связи с Банком по Системе ДБО.
- 5.3. После идентификации и аутентификации Клиент получает доступ к Системе ДБО и начинает работу с ней.
- 5.4. Клиент запрашивает и получает выписки, служебные сообщения, а также иную информацию, адресованную ему Банком.
- 5.5. Клиент запрашивает информацию и заполняет формы электронных документов и справочников, а Банк, осуществляет проверку правильности их заполнения и либо выдает служебные сообщения об ошибках, либо сохраняет переданные документы, записи справочников.
- 5.6. Уполномоченные лица Клиента подписывают электронные документы электронной подписью. Электронная подпись подтверждает авторство отправленного по Системе ДБО документа и гарантирует его целостность, т.к. любое изменение в документе после его подписания делает электронную подпись некорректной.
- 5.7. Основанием для принятия к исполнению Банком переданного Клиентом по Системе ДБО платежного документа является наличие подтверждения на исполнение ЭПД в виде необходимого количества корректных ЭП данного ЭД, а также соответствие ЭПД требованиям к оформлению платежных документов.

- 5.8. Проверка корректности ЭД осуществляется Банком в следующем порядке:
- ЭД Клиента, поступивший в ЦАП, автоматически расшифровывается и проходит автоматическую проверку на наличие и подлинность (корректность) зарегистрированных ЭП Клиента;
 - при положительном результате расшифрования ЭД и проверки ЭП электронный документ передается в Систему ДБО для дальнейшей обработки;
 - при передаче ЭПД в Систему ДБО происходит автоматическая проверка его реквизитов и, если Система ДБО не фиксирует ошибки, ЭПД передается в автоматизированную банковскую систему (АБС) Банка для исполнения.
- При отрицательном результате одной из проверок Банк не принимает ЭД и формирует для Клиента соответствующее сообщение об ошибке.
- 5.9. Принятый к исполнению Банком ЭПД подлежит исполнению в порядке проведения расчетных операций, предусмотренных соответствующим Договором банковского счета / иным договором.
- 5.10. В случае отрицательного результата какой-либо проверки Клиент получает об этом служебное электронное сообщение. Система ДБО автоматически отражает сведения о текущем состоянии документов Клиента в Банке (получении, приеме к исполнению и исполнении или неисполнении документа) посредством изменения статусов электронных документов.
- 5.11. Информация по электронным документам, оформленным с нарушением требований, размещается Банком в Системе ДБО с указанием причины, по которой не принят документ.
- 5.12. По отдельным платежным документам Банк вправе запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе ДБО, либо иным образом в день получения платежного документа. В этом случае платежный документ принимается к исполнению после получения требуемого подтверждения.
- 5.13. Электронный документ валютного контроля передается и принимается в соответствии с требованиями валютного законодательства Российской Федерации в области валютного регулирования и валютного контроля.
 Датой принятия/отправления электронного документа валютного контроля является дата его получения/направления Банком, зафиксированная Системой ДБО.
 Отказ в принятии электронного документа валютного контроля по причине несоответствия направленных документов требованиям валютного законодательства направляется Клиенту в сроки, установленные нормативными актами органов валютного контроля.
- 5.14. Информирование Клиента о совершенных с использованием Системы ДБО операциях осуществляется путем автоматического направления Банком уведомлений по Системе ДБО об изменениях статуса каждого платежного документа.

6. Порядок разрешения споров и рассмотрения претензий.

6.1. Порядок разрешения споров относительно подлинности электронных документов.

- 6.1.1. Разрешение споров относительно подлинности ЭД осуществляется на основании результатов проверки ЭП Клиента под электронным документом. Электронный документ Клиента считается подлинным, если он надлежащим образом оформлен, снабжен необходимым количеством корректных ЭП и размещен Клиентом в Системе ДБО.
- 6.1.2. Оспаривающий подлинность электронного документа Клиент направляет в Банк обоснованную претензию в письменном виде,
- 6.1.3. По результатам рассмотрения претензии Банк предоставляет Клиенту ответ в письменном виде в течение 15 (пятнадцати) рабочих дней со дня получения претензии.
- 6.1.4. В случае согласия Банка с полученной претензией, Стороны проводят переговоры по урегулированию разногласий.
- 6.1.5. В случае несогласия Банка с полученной претензией в отношении подлинности ЭД и письменного требования Клиента о создании Экспертной комиссии Банк письменно сообщает Клиенту контактную информацию своего представителя, уполномоченного представлять интересы Банка в Экспертной комиссии. Такая информация указывается в ответе на претензию либо направляется Клиенту в течение 3 (трех) рабочих дней с даты получения требования от Клиента о создании Экспертной комиссии.

- 6.1.6. Неполучение в установленный срок Клиентом ответа на претензию признается Сторонами как несогласие Банка с претензией.
- 6.1.7. Экспертная комиссия создается Сторонами в течение 3 (трех) рабочих дней со дня получения Клиентом информации о представителе, уполномоченного представлять интересы Банка в Экспертной комиссии. В указанный срок Клиент обязан уведомить Банк о назначении своего представителя, уполномоченного представлять интересы Клиента в Экспертной комиссии, предоставить в Банк его контактные данные и организовать участие в экспертизе представителя фирмы-изготовителя программного обеспечения средств ЭП - Председателя Экспертной комиссии. Оплата услуг производится Клиентом с последующим отнесением расходов на виновную сторону.
- 6.1.8. В случае если одна из Сторон не назначает представителя в Экспертную комиссию в установленный срок либо иначе уклоняется от участия в работе Экспертной комиссии, Экспертная комиссия создается при участии двух представителей фирмы-изготовителя программного обеспечения средств ЭП, причем участие одного из представителей фирмы-изготовителя программного обеспечения осуществляется за счет Стороны, уклоняющейся от участия в Экспертной комиссии независимо от результатов разрешения спора.
- 6.1.9. Стороны по требованию Экспертной комиссии предоставляют ей документы и сведения, необходимые последней для разрешения спора.
- 6.1.10. Экспертная комиссия осуществляет свою работу на территории Банка с использованием эталонной ПЭВМ (персональный компьютер, свободный от вирусов), эталонного программного обеспечения.
- 6.1.11. Эталонное оборудование и программное обеспечение предоставляется Банком. Эталонное программное обеспечение состоит из операционной системы, программного обеспечения средств ЭП, применяемых в Системе ДБО, и программного обеспечения Системы ДБО. По требованию Клиента программное обеспечение средств ЭП и Системы ДБО может предоставляться разработчиками.
- 6.1.12. Представитель Банка предоставляет документы, являющиеся надлежащими доказательствами соответствующих фактов при рассмотрении споров:
- Акт о начале использования Системы ДБО;
 - спорный ЭД в виде файла, экспортированного из базы данных входящих ЭД, а также протоколы работы Системы ДБО;
 - электронные Карточки регистрации действующих Ключей проверки электронной подписи;
 - Акт признания ключа проверки электронной подписи;
 - Заявления на конфигурирование АРМ Системы ДБО;
 - Заявления о компрометации ключей системы защиты информации;
 - журналы работы Системы ДБО, в которых отражены моменты принятия Карточки регистрации Ключа проверки электронной подписи Уполномоченного лица Клиентом;
 - полученную претензию Клиента и ответ Банка по результатам ее рассмотрения;
 - иные документы при необходимости.
- 6.1.13. Представитель Клиента предоставляет следующие документы, являющиеся надлежащими доказательствами соответствующих фактов при рассмотрении споров:
- Заявления на конфигурирование АРМ Системы ДБО с отметками Банка о принятии;
 - Заявления о компрометации ключей системы защиты информации с отметками Банка о принятии;
 - документы, свидетельствующие о расторжении Соглашения;
 - иные документы при необходимости.

В присутствии членов Экспертной комиссии представитель Банка инсталлирует эталонное программное обеспечение на эталонную ПЭВМ.

- 6.1.14. Экспертная комиссия убеждается в работоспособности компьютера и программного обеспечения и производит действия по разрешению спора, на основании которых принимает решение относительно подлинности электронных документов.
- 6.1.15. Экспертная комиссия оформляет свое решение в виде акта, который подписывается лично всеми членами комиссии и вручается под роспись уполномоченного лица Клиенту и Банку или направляется путем почтового сообщения с уведомлением о вручении.
- 6.1.16. Акт комиссии является окончательным и пересмотру не подлежит. Решение, содержащееся в акте, обязательно для исполнения обеими Сторонами. В случае уклонения какой-либо Стороны от исполнения решения, содержащегося в Акте, другая Сторона может потребовать исполнения такого решения через Арбитражный суд Российской Федерации.

6.2. Порядок разрешения споров, связанных с совершением расчетных операций с использованием Системы ДБО без согласия Клиента.

- 6.2.1. При оспаривании расчетной операции, совершенной с использованием Системы ДБО без согласия Клиента (неуполномоченным лицом), Клиент предоставляет в Банк Заявление об использовании ключей защиты информации без согласия Клиента по форме Приложения № 9 к Соглашению с приложением Справки по факту инцидента информационной безопасности в Системе ДБО (далее – Претензия).
- 6.2.2. При получении Претензии Банк:
- предпринимает предусмотренные законодательством меры по возврату денежных средств путем обращения в банк-получателя;
 - проводит внутреннее расследование, в том числе производит идентификацию оспоренного электронного документа в Системе ДБО и проверяет его подлинность.
- 6.2.3. По результатам рассмотрения Претензии и предпринятых действий Банк предоставляет Клиенту ответ в письменном виде в течение 15 (пятнадцати) рабочих дней со дня получения Претензии.

7. Порядок проверки подлинности электронного документа.

- 7.1. Установление факта соответствия спорного ЭД, представленного Банком, предмету спора.
- 7.2. Установление круга лиц, уполномоченных Клиентом на подписание ЭП спорного ЭД на момент генерации ЭП спорного ЭД.
- 7.3. Проверка соответствия принадлежности ключей проверки электронной подписи Клиента, предоставленных Банком для проведения проверки, перечню Уполномоченных лиц.
- 7.4. Проверка действительности представленных Банком ключей проверки электронной подписи Клиента на момент выработки каждой ЭП.
- 7.5. Проверка корректности ЭП спорного ЭД.
- 7.6. Установление соответствия всех ЭП спорного ЭД их заявленному назначению (ЭП группы А, ЭП группы Б, единственная ЭП).
- 7.7. Установление соответствия шестнадцатеричных значений задействованных в проверке ключей проверки электронной подписи Клиента с соответствующими значениями, указанными в Актах признания.
- 7.8. Спорный электронный документ признается подлинным тогда и только тогда, когда одновременно выполнены все условия:
- Банком представлен ЭД, соответствующий предмету спора;
 - ключи проверки электронной подписи Клиента, предоставленные Банком для проведения проверки, зарегистрированы за Уполномоченными лицами;
 - ключи проверки электронной подписи действовали в момент генерации соответствующих ЭП, т.е. на момент исполнения спорного ЭД в Банк не поступало Заявлений о компрометации соответствующих ключей защиты информации;
 - спорный ЭД содержит необходимое количество ЭП согласно их назначению;
 - все ЭП спорного ЭД корректны;

- шестнадцатеричные значения задействованных ключей проверки электронной подписи Клиента соответствуют значениям, указанным в Актах признания.

8. Особенности функционирования подсистемы Системы ДБО.

8.1. Интернет Клиент-Банк

- 8.1.1. Клиент устанавливает программное обеспечение подсистемы «Интернет Клиент Банк», представляющее собой набор элементов ActiveX, а также средства криптографической защиты информации на своем компьютере. Все электронные документы совместно с ЭП хранятся в системе управления базами данных (СУБД) Банка. СУБД на стороне Клиента не устанавливается.
- 8.1.2. При подключении к подсистеме Клиенту предоставляется 1 (один) комплект криптографических ключей: с правом единственной подписи или с разделенными правами ЭП групп А и Б.
- 8.1.3. В целях обеспечения возможности одновременного использования подсистемы разными Уполномоченными лицами по заявке Клиента Банк предоставляет дополнительные рабочие места (логины).
- 8.1.4. При подключении к подсистеме Клиент должен соблюдать следующие способы обеспечения дополнительной безопасности:
 - фильтрация подключений Клиента - Клиент указывает параметры подключения Клиента (внешние IP-адреса, MAC адреса), подлежащие контролю со стороны Банка,
 - использование дополнительных средств аутентификации по одноразовым паролям - Клиент получает по одному брелоку ОТП на каждый используемый им криптографический ключ единственной подписи либо подписи группы А.
- 8.1.5. При контроле Банком параметров подключения Клиента (внешние IP-адреса, MAC адреса) Банк разрешает только соединения, параметры которых соответствуют заявленным Клиентом в Приложении № 3 к Соглашению.
- 8.1.6. При использовании дополнительных средств аутентификации по одноразовым паролям (ОТП) при отказе от ввода такого пароля Клиент получает доступ в подсистему с ограниченными правами – не разрешена генерация ЭП электронных документов. При этом в целях использования каждого зарегистрированного брелока ОТП Банк предоставляет Клиенту отдельное рабочее место (логин).
- 8.1.7. Для создания ЭД Клиент устанавливает сеанс связи с Банком, аутентифицируется в Системе ДБО при помощи пароля и ключа подписи, производит действия по созданию, получению ЭД, выработке ЭП созданных ЭД. Все сохраненные Клиентом ЭД, а также их ЭП сохраняются в базе данных Банка.
- 8.1.8. ЭД, снабженный необходимым количеством ЭП Клиента, поступает в обработку в Банке после выполнения Клиентом необходимых действий по его передаче к исполнению.
- 8.1.9. В случае указания в Заявлении на конфигурирование АРМ необходимости предоставления доступа к счёту в режиме «только просмотр» Банк блокирует возможность управления данным счётом через указанные в Заявлении подсистемы ДБО.
- 8.1.10. Банк принимает документы, передаваемые Клиентом через информационно-коммуникационную сеть Интернет, а также размещает всю необходимую информацию в персонализированном разделе веб сервера Системы ДБО в автоматическом режиме. Данный раздел доступен Клиенту после прохождения процедуры авторизации.
- 8.1.11. Банк обязан размещать всю информацию, предназначенную для получения Клиентом в подсистеме на персонализированной странице интернет-сервера Системы ДБО.
- 8.1.12. Информация по электронным документам, оформленным с нарушением требований, размещается Банком на интернет-сервере Системы ДБО в день получения переданного Клиентом на исполнение документа, с указанием причины, по которой документ не принят.
- 8.1.13. Поток всех передаваемых между Клиентом и Банком данных шифруется с помощью протокола SSL.

- 8.1.14. Установление соединения производится Клиентом. Адрес сервера Банка: <https://dbo.bank-peresvet.ru>.
- 8.1.15. Количество разрешенных одновременных соединений Клиента с сервером ДБО Банка определяется числом лицензий, запрошенных Клиентом в Заявке на подключение Системы ДБО.
- 8.1.16. Системой ДБО могут присваиваться следующие статусы ЭД Клиента:

Статус ЭД	Описание статуса
новый	вновь созданный или импортированный документ, успешно прошедший проверку всех контролей Системы ДБО
импортирован	статус присваивается импортированному из бухгалтерской системы (БС) документу, в котором были обнаружены ошибки
подписан	документ подписан всеми требуемыми подписями
подписан I	документ подписан ЭП группы А из двух требуемых
подписан II	документ подписан ЭП группы Б из двух требуемых
в обработке	документ принят Системой ДБО со стороны Банка, производится его передача в АБС
ожидает визирования	обработка системного документа приостановлена до его подписания / отказа в подписании визирующей подписью
принят АБС	документ успешно прошел проверку всех контролей АБС и передан на исполнение операционисту
отказан АБС	документу, переданному в АБС, отказано в исполнении, обоснование отказа можно увидеть в поле «Сообщение банка» (Комментарий банка) при просмотре документа
исполнен	документ исполнен
не принят	документу отказано в визировании визирующей подписью
удален	документ был удален

Приложение № 2
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

Требования подсистем ДБО к программным, техническим средствам, каналам связи

1 Интернет Клиент-Банк

- 1.1 Требования к программным и техническим средствам, приобретаемым Клиентом за собственный счет у третьих лиц:
- 1.1.1 Подсистема может устанавливаться на одну или несколько рабочих станций Уполномоченных лиц, осуществляющих работу с Системой ДБО.
- 1.1.2 На рабочих станциях должна быть установлена операционная система: Windows 7 x86 и x64 (Ultimate, Professional, Enterprise, Home Premium, Home Basic), Windows 8 x86 и x64 (Windows 8, Windows 8 Pro, Windows 8 Enterprise), Windows 10 x86 и x64 (Home, Professional, Enterprise).
- 1.1.3 На рабочих станциях должно быть установлено программное обеспечение: Microsoft Office 2003, 2007 или 2010 с компонентами – MS Word, MS-Excel.
- 1.1.4 Интернет браузер: MS Internet Explorer x86, x64 версии 11.0, Mozilla Firefox x86 v.51.0.1, Opera x86 v.43.0.2442, Google Chrome x86 v.56.0.
- 1.1.5 На рабочие станции устанавливается программное обеспечение подсистемы «Интернет Клиент-Банк» Системы ДБО.
- 1.1.6 Используемые рабочие станции должны быть полностью совместимы с установленной операционной системой. Гарантией такой совместимости является логотип Windows Logo Basic.
- 1.1.7 На рабочие станции устанавливается программное обеспечение средства криптографической защиты информации КристоПро CSP:
- При использовании ОС Windows 7/ Windows 8 x86 и x64 (Ultimate, Professional, Enterprise, Home Premium, Home Basic): КристоПро CSP версии 3.9 или КристоПро CSP версии 4.0
 - При использовании ОС Windows 10 x86 и x64 (Home, Professional, Enterprise): КристоПро 3.9 R2' или КристоПро CSP версии 4.0
- 1.1.8 Дистрибутив средства криптографической защиты информации может быть загружен с сайта Банка (<http://www.bank-peresvet.ru/dbo/>) или получен в Банке на материальном носителе. Вместе с дистрибутивами СКЗИ на сайте Банка размещаются контрольные суммы установочных модулей и документации. Контрольные суммы рассчитываются в соответствии с ГОСТ Р 34.11 94 с учётом RFC 4357, а также md5.
- В случае загрузки средства криптографической защиты информации с сайта, должна быть осуществлена проверка целостности полученных установочных модулей СКЗИ и эксплуатационной документации. Проверка должна быть осуществлена с помощью утилиты `srverify.exe`, входящей в состав СКЗИ «КристоПро CSP» `srverify -mk <filename>`, либо иным другим сертифицированным ФСБ России шифровальным (криптографическим) средством, реализующим ГОСТ Р 34.11-94. Контрольная сумма md5 может быть проверена с помощью `md5sum (linux)` или `File Checksum Integrity Verifier (http://support.microsoft.com/kb/841290)`.
- 1.1.9 Аппаратная конфигурация рабочих станций должна предусматривать наличие не менее 100 Мб свободной памяти на жестком диске компьютера и не менее 512 Мб (рекомендуется 1 Гб) оперативной памяти, а также или USB порта для работы со съемными носителями информации, содержащими криптографические ключи. В качестве ключевых носителей могут быть использованы только съемные носители (или USB Flash).
- 1.1.10 Принтер.
- 1.2 Лица, осуществляющие настройку и обновление Системы ДБО, должны иметь права администратора рабочей станции.
- 1.3 Требования к подключению.

- 1.3.1 Для подключения к серверу Банка необходимо установить соединение с сервером Банка <https://dbo.bank-peresvet.ru> через информационно-телекоммуникационную сеть Интернет. В процессе работы с сервером используются порты tcp 80, tcp 443.
- 1.3.2 Соединение может быть как постоянным, так и коммутируемым.
- 1.3.3 Пропускная способность канала связи должна быть обеспечена на уровне не ниже 512 Кбит/с, а комфортная работа гарантируется при пропускной способности канала 1 Мбит/с.

Приложение № 3
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

заполненный в формате Word бланк распечатывается с двух сторон на одном листе

<input type="checkbox"/> Первичное	<input type="checkbox"/> Повторное
------------------------------------	------------------------------------

Заявление на конфигурирование АРМ Системы ДБО BS-Client v.3

Наименование Клиента

ИНН

1. Перечень счетов Клиента, обслуживаемых в Системе ДБО:

Подключить	Отключить	Только просмотр	Визирование	Номера счетов:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

2. Перечень подсистем Системы ДБО, действия по настройке:

Подключить	Отключить	Название подсистемы
<input type="checkbox"/>	<input type="checkbox"/>	Интернет Клиент-Банк
Восстановление работоспособности АРМ:		
<input type="checkbox"/> с восстановлением начальных настроек ключей		<input type="checkbox"/> повторное включение заблокированного АРМ
Действия по настройке Системы ДБО		
<input type="checkbox"/> предоставление дополнительных лицензий СКЗИ КриптоПро CSP: ____ штук		
<input type="checkbox"/> предоставление брелоков OTP взамен утраченных: ____ штук		
<input type="checkbox"/> предоставление дополнительных подключений (логинов) Интернет Клиент-Банк: ____ штук		

3. Объединение АРМ Клиента с общим АРМ / выделение АРМ Клиента из общего АРМ*:

Наименования прочих Клиентов единого АРМ Номер общего АРМ: _____	Объединить	Выделить
	<input type="checkbox"/>	<input type="checkbox"/>

* - производится со сменой ключей и заполнением раздела 4 заявления. Ключи клиентов общего АРМ не меняются.

4. Список Уполномоченных лиц, прав подписи (режимов ЭП)

Добавить	Отозвать	Приостановить	ФИО Уполномоченного лица	Права подписи*	Подключение (логин)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

* Допустимые варианты прав подписи (режима ЭП): Единственная, ЭП группы А, ЭП группы Б, Без права подписи

5. Безопасность доступа Клиента

Разрешить	Отключить	ФИО Уполномоченного лица / логин	MAC адреса АРМ	Внешние IP-адреса, сети, диапазоны
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	<input type="checkbox"/>			
Безопасность Клиента при использовании подсистемы «Интернет Клиент-Банк»				
<input type="checkbox"/> использовать брелоки для генерации одноразовых паролей (OTP) Интернет Клиент-Банка				
<input type="checkbox"/> синхронизация счетчика брелока (OTP) Интернет Клиент-Банка с разблокировкой логина				
<input type="checkbox"/> смена пароля* для логина _____			<input type="checkbox"/> замена логина _____	

* При смене пароля для заблокированного логина автоматически выполняется разблокирование логина

6. Контактная информация: _____

7. Получение: в офисе Банка на адрес электронной почты _____

8. Перечень счетов Клиента _____ (АРМ _____), подлежащих визированию:

Визирование	Номера счетов:
<input type="checkbox"/>	
<input type="checkbox"/>	

9. Дополнительные сведения: _____

Руководитель: _____ / _____ /

М.П.

(заполняется Банком)

АРМ: _____ Договор № _____

Дополнительные сведения: _____

Принято Банком:

_____ / _____ /

должность уполномоченного сотрудника

ФИО

подпись

« _____ » _____ 20__ г.

Приложение № 4
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

Акт приема-передачи

Акционерный коммерческий банк содействия благотворительности и духовному развитию Отечества «ПЕРЕСВЕТ» (Акционерное общество), в лице _____, действующего на основании _____, именуемое в дальнейшем «Банк», с одной стороны, и _____, в лице _____, действующего на основании _____, именуем__ в дальнейшем «Клиент», с другой стороны, составили настоящий Акт о выполнении указанных ниже действий с учётом ограничений подключаемых Клиентом подсистем Системы ДБО:

1. Банк передал Клиенту, а Клиент принял от Банка:

- дистрибутивные копии программного обеспечения Системы ДБО,
- документацию на программное обеспечение Системы ДБО,
- необходимые для использования Системы ДБО логины и пароли Клиента,
- дистрибутивные копии и серийные номера программного обеспечения средства криптографической защиты информации КриптоПро CSP в количестве штук: _____ (_____),
- документацию на программное обеспечение средств криптографической защиты информации,
- брелоки для генерации одноразовых паролей в количестве штук: _____ (_____).

2. Настоящий Акт составлен в 2 (двух) экземплярах по одному для каждой из сторон и является неотъемлемой частью Соглашения.

От Банка:

_____/_____

_____/_____

От Клиента:

«_____» _____ 20__ г.

Приложение № 5
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

АКТ ПРИЗНАНИЯ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

—
наименование Клиента (режим подписи)

Сведения о Клиенте – юридическом лице:

1. ИНН, Наименование организации/ФИО индивидуального предпринимателя: _____
2. Место нахождения/адрес регистрации индивидуального предпринимателя: _____
3. Почтовый адрес: _____
4. Тел. _____ 5. Факс _____ 6. e-mail _____

Сведения об Уполномоченном лице:

1. Фамилия, имя, отчество: _____
2. Должность: _____
3. документ, удостоверяющий личность: паспорт _____ выдан «__» _____ 20__
г. _____

Личная подпись Уполномоченного лица _____

Параметры ключа:

Номер Клиента:	
Дата изготовления:	

Рекомендуемый срок плановой смены: в течении 3 месяцев по истечении 1 года с момента изготовления.

Текст ключа проверки электронной подписи:

Указанное Уполномоченное лицо имеет право использовать ЭП в электронных документах, передаваемых в Банк от имени Клиента.

Достоверность приведенных данных подтверждаем

«__» _____ 20__ г.

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

Приложение № 6
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

Акт о начале использования Системы ДБО

Акционерный коммерческий банк содействия благотворительности и духовному развитию Отечества «ПЕРЕСВЕТ» (Акционерное общество), в лице _____, действующего на основании _____, именуемое в дальнейшем «Банк», с одной стороны, и _____, в лице _____, действующего на основании _____, именуемый в дальнейшем «Клиент», с другой стороны, составили настоящий Акт о выполнении указанных ниже действий для следующих подключаемых Клиентом подсистем Системы ДБО:

1. Клиент заявляет о том, что технические и программные средства Клиента соответствуют требованиям используемых подсистем Системы ДБО.
2. Клиент ознакомился с документацией на Систему ДБО и используемые средства криптографической защиты информации.
3. Клиент обучен условиям, правилам и методам эксплуатации Системы ДБО и используемых средств криптографической защиты информации.
4. На технических средствах Клиента произведена установка и настройка необходимых программных средств используемых подсистем Системы ДБО.
5. Клиентом с помощью Системы ДБО успешно произведен тестовый сеанс связи.
6. Для подсистем Системы ДБО, использующих СКЗИ:
 - 6.1 Клиент предоставил все необходимые документы на лиц, уполномоченных распоряжаться денежными средствами Клиента, с использованием ЭП.
 - 6.2 Клиентом с помощью Системы ДБО успешно произведена генерация рабочих криптографических ключей системы защиты информации.
 - 6.3 Клиент передал Банку заполненные и заверенные подписью и печатью Клиента Акты признания ключей проверки электронной подписи Клиента.
 - 6.4 Банк изготовил Карточки регистрации Ключей проверки электронной подписи рабочих ключей Клиента, осуществил ввод в действие рабочих ключей Клиента и передал Клиенту соответствующие им Карточки регистрации Ключей проверки электронной подписи.
7. Дата и время начала эксплуатации подключаемых Клиентом подсистем Системы ДБО «_____» _____ 20__ г. 09:00.
8. Настоящий Акт составлен в 2 (двух) экземплярах по одному для каждой из сторон и является неотъемлемой частью Соглашения.

От Банка:

_____/_____

_____/_____

От Клиента:

«_____» _____ 20__ г.

Приложение № 7
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

Заявление о компрометации ключей системы защиты информации

1. Клиент настоящим заявляет о компрометации криптографических ключей следующих Уполномоченных лиц Клиента:

ФИО Уполномоченного лица	Режим подписи*

* Допустимые варианты: Единственная, ЭП группы А, ЭП группы Б, Без права подписи

Причина компрометации:

- увольнение/смена сотрудника, имевшего доступ к ключевому носителю
- потеря ключевого носителя (в т.ч. с последующим нахождением)
- смена владельца ключа
- выявление воздействия вредоносного программного обеспечения (вируса)
- попытка хищения средств (в т.ч. в других банках с использованием данного ПК или с другого ПК, к которому подключался ключевой носитель)

Дополнительно могу сообщить _____

Руководитель: _____ / _____ /

М.П.

Принято Банком:	(заполняется Банком)
<div style="display: flex; justify-content: space-between; border-top: 1px solid black; border-bottom: 1px solid black;"> _____ / _____ / </div> <div style="display: flex; justify-content: space-between; font-size: small;"> должность уполномоченного сотрудника подпись ФИО </div>	
заявление принято в ____:____ московского времени « ____ » _____ 20__ г.	
Версия ДБО _____	АРМ _____

Приложение № 9
к Правилам АКБ «ПЕРЕСВЕТ» (АО)

по использованию Системы дистанционного банковского обслуживания BS-Client v.3

**ЗАЯВЛЕНИЕ ОБ ИСПОЛЬЗОВАНИИ КЛЮЧЕЙ ЗАЩИТЫ ИНФОРМАЦИИ
БЕЗ СОГЛАСИЯ КЛИЕНТА**

В АКБ «ПЕРЕСВЕТ» (АО)

от _____

«___» _____ 20__ года с расчетного счета _____, открытого в АКБ «ПЕРЕСВЕТ» (АО), по системе дистанционного банковского обслуживания неустановленным лицом 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: _____¹

Прошу Вас заблокировать учетную запись в Системе ДБО и оказать содействие в возврате денежных средств.

Прилагаю Справку по факту инцидента информационной безопасности в Системе ДБО на _____ листах.

должность

подпись

расшифровка подписи

«___» _____ 20__

Исп. _____
Фамилия И.О.

¹ Для случаев перевода электронных денежных средств – указать реквизиты перевода.

СПРАВКА ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДБО

Дополнительно сообщая:

Количество электронных устройств (ЭУ), настроенных для доступа в Систему ДБО:

_____.

Для доступа в Систему 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 информационно-телекоммуникационной сети Интернет
- с ЭУ разрешены исходящие соединения с Банком и ограниченным числом сайтов информационно-телекоммуникационной 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: _____

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 № _____ 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 нелегализованного и контрафактного программного обеспечения в соответствии со статьей 146 Уголовного кодекса Российской Федерации предупрежден.

должность

подпись

расшифровка подписи

« ____ » _____ 20__