

**УТВЕРЖДЕНО**

Решением Правления  
АКБ «АПАБАНК» (ЗАО)  
(Протокол № 12/1 от «16» августа 2013г.)

## **РЕГЛАМЕНТ**

**РЕАЛИЗАЦИИ АКБ «АПАБАНК» (ЗАО)**

**ФУНКЦИЙ**

**УДОСТОВЕРЯЮЩЕГО ЦЕНТРА**

## Содержание

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
2. ОБЩИЕ ПОЛОЖЕНИЯ.....	4
3. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА БАНКА.....	5
4. ПРАВА И ОБЯЗАННОСТИ СТОРОН.....	8
5. ОТВЕТСТВЕННОСТЬ СТОРОН.....	9
6. РАЗРЕШЕНИЕ СПОРОВ И КОНФЛИКТНЫХ СИТУАЦИЙ.....	10
7. ПРИЛОЖЕНИЯ.....	11

## 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Администратор безопасности системы** – работник Отдела автоматизации - подразделения Банка, наделенный полномочиями по регистрации и управлению сертификатами ключей подписей Пользователей Удостоверяющего Центра Банка и уполномоченный расписываться собственноручной подписью на бланках сертификатов ключей подписей, изданных Удостоверяющим Центром Банка.

**Банк** – АКБ «АПАБАНК» (ЗАО).

**Владелец сертификата ключа проверки электронной подписи** - физическое лицо, на имя которого Удостоверяющим Центром выдан сертификат ключа проверки электронной подписи, и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

**Договор на обслуживание в системе электронного документооборота Банка** - договор, заключенный между Клиентом и Банком на обслуживание в системе электронного документооборота Банка.

**Ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи

**Ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

**Ключевой носитель** – физический носитель информации, содержащий ключевую информацию. К основным типам ключевых носителей относятся: USB-token, SMART-CART.

**Компрометация ключей** - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- Утрата персонального аппаратного криптопровайвера;
- Утрата персонального аппаратного криптопровайвера с последующим обнаружением;
- Увольнение сотрудников, имевших доступ к ключевой информации;
- Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;
- Возникновение подозрений в утечке информации или ее искажении в системе конфиденциальной связи;
- Случаи, когда нельзя достоверно установить, что произошло с персональным аппаратным криптопровайдером, содержащим ключевую информацию (в том числе случаи, когда персональный аппаратный криптопровайдер вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

**Пользователь Удостоверяющего центра Банка** - юридическое лицо, зарегистрированное в Удостоверяющем Центре Банка и являющееся участником системы электронного документооборота Банка.

**Рабочий день Удостоверяющего центра Банка** – промежуток времени 9:30 -18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

**Реестр Удостоверяющего центра Банка** – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на аннулирование ключей подписей;
- реестр заявлений на приостановление/возобновление действия ключей подписей;
- реестр заявлений на подтверждение подлинности электронной цифровой подписи в электронном документе;
- реестр сертификатов ключей проверки электронной подписи

**Система электронного документооборота Банка (СЭД Банка)** – организационно-техническая система обмена электронными документами, представляющая собой совокупность программного, аппаратного и программно-

аппаратного обеспечения участников системы, правовой статус которой определен владельцем этой системы или соглашениями между ее участниками.

**Средства Удостоверяющего центра Банка** – программные и аппаратные средства, используемые для реализации функций удостоверяющего центра.

**Сертификат ключа проверки электронной подписи сотрудника клиента в системе «iBank2»**– документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью Уполномоченного лица Удостоверяющего Центра Банка, Администратора Безопасности системы и печатью Банка.

**Средство криптографической защиты информации (СКЗИ)** – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

**Средства электронной подписи** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

**Удостоверяющий центр Банка (УЦ Банка)** – совокупность технических и организационных средств, локализованных в Отделе автоматизации АКБ «АПАБАНК» (ЗАО), и, позволяющая осуществлять АКБ «АПАБАНК» (ЗАО) функций по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим регламентом и Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

**Уполномоченное должностное лицо Банка** – физическое лицо – работник Банка, осуществляющий регистрацию сертификатов ключей подписей Пользователей Удостоверяющего Центра Банка, а так же уполномоченный расписываться собственноручной подписью на бланках сертификатов ключей подписей, изданных Удостоверяющим Центром Банка.

**Усиленная неквалифицированная электронная подпись** – электронная подпись, которая:

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

**Участники электронного взаимодействия** – Банк и его Клиенты, осуществляющие обмен информацией в электронной форме Банк и его Клиент.

**Электронный документ** - документ, информация в котором представлена в электронной форме.

**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.

## **2. ОБЩИЕ ПОЛОЖЕНИЯ**

2.1. Настоящий Регламент Удостоверяющего Центра Банка, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, отношения в области использования электронных подписей при совершении гражданско-правовых сделок и при совершении иных юридически значимых действий, а именно:

В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Приказом Федеральной службы безопасности РФ от 27 декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи», Приказом Федеральной службы безопасности РФ от 27 декабря 2011 года № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра», Приказом ФСБ от 9 февраля 2005 г. № 66 «Об утверждении

положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение пкз-2005)», Приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

2.2. Удостоверяющий Центр Банка (далее по тексту – УЦ Банка) осуществляет свою деятельность в соответствии с Федеральным законом от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» и Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» на основании следующих лицензий:

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 9703 Р от 09 ноября 2010 г. на право осуществлять деятельность по распространению шифровальных (криптографических) средств;

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 9702 Х от 09 ноября 2010 г. на право осуществлять деятельность по техническому обслуживанию шифровальных (криптографических) средств;

Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 9704 У от 09 ноября 2010 г. на право осуществлять предоставление услуг в области шифрования информации.

2.3. Настоящий Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации, т.е. путем присоединения к Регламенту в целом, с учетом условий и оговорок, которые изложены в приложениях к настоящему Регламенту.

2.4. Сторонами Регламента (далее - Стороны) являются УЦ Банка и Пользователь УЦ Банка.

2.5. Настоящий Регламент определяет условия предоставления и правила пользования услугами УЦ Банка, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно -технические мероприятия, направленные на обеспечение работы УЦ Банка.

2.6. Присоединение к настоящему Регламенту осуществляется путем заключения с банком Договора на обслуживание с использованием системы «БАНК-КЛИЕНТ».

2.7. Нормы, содержащиеся в Регламенте, становятся обязательными для исполнения Сторон с момента заключения Клиентом Договора на обслуживание в системе электронного документооборота Банка. Для работника Банка с момента передачи в УЦ Банка сертификата ключа проверки электронной подписи сотрудника клиента в системе «iBank 2».

2.8. Банк имеет право в одностороннем порядке вносить изменения и дополнения в Регламент. Уведомление о внесении изменений или дополнений в Регламент и уточненная редакция Регламента размещаются на Интернет странице Банка в разделе УЦ, расположенной по адресу <http://www.apabank.ru> не позднее, чем за 10 (десять) календарных дней до вступления изменений и дополнений в силу.

2.9. Действия настоящего Соглашения может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- нарушением одной из Сторон условий настоящего Регламента.

В случае расторжения Соглашения инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за тридцать календарных дней до даты расторжения Соглашения. Стороны осуществляют окончательные взаиморасчеты в течение 10 (Десяти) дней с даты расторжения Соглашения.

Прекращение действия Соглашения не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Соглашения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

2.10. Настоящий Регламент вступает в силу со дня его утверждения решением Правления Банка.

### **3. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА**

### **3.1. Регистрация Пользователей Удостоверяющего Центра Банка.**

Удостоверяющий центр Банка осуществляет регистрацию Пользователя в Удостоверяющем Центре Банка только в том случае, если Клиент присоединился к Регламенту, в соответствии с п. 2.6 настоящего Регламента.

Порядок регистрации пользователей СЭД Банка в УЦ Банка определяется Договором на обслуживание с использованием системы «БАНК-КЛИЕНТ», который описывает процедуры регистрации Пользователей, генерации ключей, управления сертификатами ключей.

После осуществления регистрации УЦ предоставляет Пользователю:

- ключевой носитель (usb-токен, смарт-карта)
- дополнительное средство многофакторной аутентификации Клиента OTP-токен
- криптобиблиотеку СКЗИ «Крипто-КОМ 3.2» компании «Сигнал-КОМ»
- документацию по настройке и использованию системы «iBank2».

### **3.2. Генерация ключей Пользователя Удостоверяющего Центра Банка.**

Порядок генерации закрытых ключей Пользователей УЦ Банка изложен в Договоре на обслуживание по системе «БАНК-КЛИЕНТ», и в общем случае включает в себя следующие этапы:

3.2.1. Генерация закрытого ключа для усиленной неквалифицированной электронной подписи создается Пользователем на своем рабочем месте с помощью СКЗИ (используя Руководство Пользователя УЦ Банка) и сохранение его на персональном ключевом носителе, поддерживаемом используемым СКЗИ. В целях противодействия получению несанкционированного доступа к закрытым ключам электронной подписи (и шифрования), ключевую информацию рекомендуется хранить на защищенных носителях (смарт-картах, USB-токенах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Краткое руководство пользователя - «Internet-Банкинг для корпоративных клиентов», Пользователь УЦ Банка получает при передаче УЦ Банка Пользователю носителя ключа проверки ЭП (Приложение №1 к Регламенту).

3.2.2. Два экземпляра копий сертификата ключа проверки усиленной неквалифицированной электронной подписи сотрудника клиента в системе «iBank2» на бумажном носителе заверяются печатью и подписывается собственноручной подписью. Затем направляется для проверки Уполномоченным работником УЦ Банка на достоверность и идентичность сведений, содержащихся в полученном сертификате.

3.2.3. Уполномоченное лицо УЦ Банка и Администратор безопасности системы заверяют сертификат ключа проверки электронной подписи клиента в системе "iBank 2". Один экземпляр возвращается Пользователю УЦ Банка, а другой остается в УЦ Банка (Приложение №7).

Юридическую силу электронная подпись приобретает только после заверения, соответствующего выпущенного сертификата ключа подписи Уполномоченным лицом УЦ Банка. Таким образом, до начала использования в работе системы ДБО Банка сертификат должен быть заверен двумя Сторонами.

3.2.4. При плановой смене ключей для усиленной неквалифицированной электронной подписи производит Пользователь на своем рабочем месте. За 30 календарных дней до окончания срока действия закрытого ключа УЦ Банка по системе ДБО уведомляет Пользователя УЦ Банка о необходимости осуществления плановой смены ключей. При внеплановой смене сертификата ключа усиленной неквалифицированной электронной подписи (при утере ключа, истечения срока действия и т.д.), основанием для выпуска нового сертификата будет являться заявление на аннулирование закрытого ключа усиленной неквалифицированной электронной подписи Пользователя УЦ Банка (с указанием причины), для создания нового сертификата (Приложение №2 к Регламенту).

### **3.3. Аннулирование ключа подписи Пользователя Удостоверяющего Центра Банка.**

УЦ аннулирует сертификат ключа подписи Пользователя УЦ Банка в следующих случаях:

- по истечению срока его действия;
- в случае прекращения действия настоящего Регламента в отношении Пользователя УЦ Банка;
- по заявлению Пользователя УЦ;
- при компрометации ключевой информации Уполномоченного лица УЦ Банка.

Для осуществления аннулирования ключа подписи Пользователь УЦ Банка подает заявление на аннулирование ключа подписи в УЦ Банка (Приложение №2 к Регламенту), в соответствии с порядком предусмотренным Договором (Соглашением) на обслуживание в СЭД Банка.

### **3.4. Приостановление действия ключа подписи Пользователя Удостоверяющего Центра Банка.**

3.4.1. УЦ Банка приостанавливает действие сертификата ключа подписи Пользователя УЦ Банка в следующих случаях:

- по заявлению Пользователя УЦ Банка;
- в случаях возникновения подозрения о компрометации ключевой информации Пользователя УЦ Банка после аутентификации Пользователя по ключевой фразе;
- в иных случаях, предусмотренных положениями настоящего Регламента по решению УЦ Банка.

3.4.2. Приостановление действия ключа подписи и официальное уведомление Пользователя УЦ Банка и всех лиц, зарегистрированных в УЦ Банка, о приостановлении действия сертификата ключа подписи, должны быть осуществлены не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в УЦ Банка (Приложение №3 к Регламенту).

3.4.3. В случае приостановления действия ключа подписи при возникновении подозрения на компрометацию ключевой информации Пользователя УЦ Банка официальное уведомление Пользователя и всех лиц, зарегистрированных в УЦ Банка, о приостановлении действия ключа должно быть осуществлено не позднее одного рабочего дня, следующего за рабочим днем, в течение которого Пользователь УЦ Банка сообщил о компрометации ключевой информации.

3.4.4. При приостановлении действия ключа подписи в случаях, предусмотренных положениями настоящего Регламента, по решению УЦ Банка, официальное уведомление о приостановлении действия сертификата должно быть осуществлено не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было принято решение о приостановлении действия сертификата.

3.4.5. В случае если, в течение срока приостановления действия ключа подписи Пользователя, в УЦ Банка не поступает заявление от пользователя СЭД Банка о возобновлении действия ключа подписи, ключ подписи аннулируется УЦ Банка.

### **3.5. Возобновление действия ключа подписи Пользователя Удостоверяющего Центра.**

3.5.1. УЦ Банка возобновляет действие сертификата ключа подписи Пользователя УЦ Банка только по заявлению Пользователя.

3.5.2. Подача заявления на возобновление действия ключа подписи Пользователя УЦ Банка осуществляется Пользователем УЦ Банка посредством почтовой или курьерской связи по форме Приложения № 4 к Регламенту.

3.5.3. Возобновление действия ключа подписи и официальное уведомление Пользователя и всех лиц, зарегистрированных в УЦ Банка, о возобновлении действия ключа подписи, должны быть осуществлены не позднее 3 рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в УЦ Банка.

3.5.4. Возобновление действия ключа по распоряжению руководства УЦ Банка.

### **3.6. Подтверждение подлинности электронной подписи в электронном документе**

3.6.1. По письменному обращению Пользователя, УЦ Банка осуществляет проведение экспертных работ по подтверждению электронной подписи в электронном документе.

Для подтверждения подлинности электронной подписи в электронном документе Пользователь УЦ Банка подает заявление на подтверждение подлинности электронной подписи в электронном документе в УЦ Банка по форме Приложения №5 к Регламенту.

**3.6.2. Электронная подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:**

3.6.2.1. сертификат ключа проверки подписи, указанный в заявлении на подтверждение подлинности электронной подписи, не утратил силу (действует) на момент формирования электронной подписи в электронном документе дата и время формирования электронной подписи в электронном документе, указанная в заявлении на подтверждение подлинности электронной подписи;

3.6.2.2. электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи сотрудника;

3.6.2.3. формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

3.6.3. Срок проведения работ по подтверждению подлинности электронной подписи в электронном документе и предоставлению заключения о произведенной проверке составляет 5 (пять) рабочих дней с момента его поступления в УЦ Банка.

3.6.4. Проведение работ по подтверждению подлинности электронной подписи в электронном документе осуществляет комиссия, состоящая не менее чем из 3-х человек, сформированная из числа работников Банка.

3.6.5. Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является Акт УЦ Банка, оформленный в письменном виде, подписанный всеми членами комиссии и заверенный печатью УЦ Банка, которая является печатью АКБ «АПАБАНК» (ЗАО) (Приложение №6 к Регламенту).

#### **3.6.6. Акт о выполненной проверке содержит:**

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные комиссии для проведения проверки.

3.6.6.1. Акт о выполненной проверке составляется в письменной форме, заверяется собственноручными подписями всех членов комиссии (Приложение №6 к Регламенту).

## **4. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

### **4.1. Удостоверяющий Центр Банка обязан:**

4.1.1. Использовать для генерации закрытого ключа электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

4.1.2. Принять меры по защите закрытого ключа Уполномоченного лица УЦ Банка от несанкционированного доступа.

4.1.3. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы или города, где располагается филиал Банка - для Доверенного ЦР. УЦ Банка обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

4.1.4. Обеспечить регистрацию Пользователей в УЦ Банка в соответствии с порядком, определенным настоящим Регламентом.

4.1.5. Внести регистрационную информацию Пользователей в Реестр УЦ Банка и обеспечить уникальность регистрационной информации всех зарегистрированных в УЦ Банка лиц, используемой для идентификации владельцев сертификатов ключей подписей.

4.1.6. Обеспечить уникальность идентификатора ключа проверки электронной подписи.

4.1.7. Аннулировать ключ подписи Пользователя УЦ Банка по заявлению на аннулирование сертификата ключа подписи в соответствии с порядком, определенным настоящим Регламентом не позднее 3-х рабочих дней с момента подачи заявления на аннулирование ключа.

4.1.8. Приостановить действие сертификата ключа подписи Пользователя УЦ Банка по заявлению на приостановление действия сертификата ключа подписи в соответствии с порядком, определенным настоящим Регламентом. Не позднее 3-х рабочих дней с момента подачи заявления на аннулирование (отзыв) сертификата.

4.1.9. Возобновить действие ключа подписи Пользователя УЦ Банка по заявлению на возобновление действия сертификата ключа подписи (в случае поступления заявления в период срока, на который действие сертификата было приостановлено) в соответствии с порядком, определенным в настоящем Регламенте.

4.1.10. Аннулировать ключ подписи лица, зарегистрированного в УЦ Банка, в случае, если истек установленный срок.

4.1.11. Аннулировать ключа подписи лица, зарегистрированного в УЦ Банка, в случае компрометации закрытого ключа Уполномоченного лица УЦ Банка, которым заверен указанный сертификат.

## **4.2. Пользователь Удостоверяющего Центра Банка обязан:**

4.2.1. Генерировать ключ проверки электронной подписи и ключ электронной подписи только с использованием средства электронной подписи и ПО, предоставленного УЦ Банка.

4.2.2. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования

4.2.3. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

4.2.4. Немедленно обратиться в УЦ Банка с заявлением на приостановление действия ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а так же в случае, если Пользователю УЦ Банка стало известно, что этот ключ используется или использовался ранее другими лицами.

4.2.5. Регулярно, не реже чем один раз одного раза в месяц, просматривать Интернет страницу Банка, раздел УЦ Банка, расположенную по адресу URL= <http://apabank.ru/about/licence/> на предмет изменения Регламента.

## **4.3. Удостоверяющий Центр Банка имеет право:**

4.3.1. Отказать в регистрации в УЦ Банка Пользователю в случае ненадлежащего оформления необходимых регистрационных документов.

4.3.2. Отказать в аннулировании ключа подписи Пользователя УЦ Банка в случае ненадлежащего оформления заявления на аннулирование ключа подписи.

4.3.3. Отказать в приостановлении/возобновлении действия ключа подписи Пользователя в случае ненадлежащего оформления заявления на приостановление/возобновление действия ключа подписи.

4.3.4. Отказать в аннулировании ключа подписи Пользователя УЦ в случае, если истек установленный срок действия.

4.3.5. Отказать в возобновлении действия ключа подписи Пользователя УЦ в случае, если истек установленный срок действия.

4.3.6. Аннулировать ключа подписи Пользователя УЦ в случае установленного факта компрометации ключевой информации, с уведомлением владельца аннулированного ключа подписи и указанием обоснованных причин аннулирования.

4.3.7. Приостановить действие ключа подписи Пользователя УЦ с обязательным уведомлением владельца сертификата ключа подписи, действие которого приостановлено, и указанием обоснованных причин приостановления.

4.3.8. Отказать в создании ключа подписи Пользователя УЦ Банка в случае, если СКЗИ использованное для формирования запроса на создание ключа подписи, не поддерживается УЦ Банка.

## **4.4. Пользователь Удостоверяющего Центра Банка имеет право:**

4.4.1. Применять сертификат ключа подписи Пользователя УЦ Банка для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

4.4.2. Генерировать ключ проверки электронной подписи и ключи электронной подписи на своем рабочем месте с использованием СКЗИ, предоставленного УЦ Банка или программного средства СЭД Банка, пользователем которой он является.

4.4.3. Воспользоваться предоставляемыми СЭД Банка, пользователем которой он является, программными средствами для передачи по каналам связи в УЦ Банка документов в электронном виде, определенных настоящим Регламентом.

4.4.4. Обратиться в СЭД Банка, пользователем которой он является, за подтверждением подлинности электронных подписей в электронных документах.

4.4.5. Обратиться в УЦ Банка с заявлением на аннулирование ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

4.4.6. Обратиться в УЦ Банка с заявлением на приостановление действия сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

## **5. ОТВЕТСТВЕННОСТЬ СТОРОН**

5.1. Размер ответственности Банка и присоединившейся Стороны при нарушении условий настоящего Регламента определяется в соответствии с Договором на обслуживание в СЭД Банка, подписанным Банком и присоединившейся Стороной.

5.2. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

5.3. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

5.4. УЦ Банка несет ответственность за убытки при использовании закрытого ключа электронной подписи и сертификата ключа подписи Пользователя УЦ Банка только в случае, если данные убытки возникли при компрометации ключевой информации Уполномоченного лица УЦ Банка.

5.5. Ответственность за регистрацию Пользователей УЦ Банка, занесению данных в сертификаты ключей подписей, изготовлению и управлению сертификатами ключей подписей, изготовлению бланков сертификатов ключей проверки электронной подписи Пользователей УЦ Банка возлагается на УЦ Банка, который обоснованно полагается на сведения, указанные в «Анкете клиента - юридического лица в случае открытия счета самим юридическим лицом» УЦ Банка.

5.6. УЦ Банка не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если сведения, указанные в заявлении на регистрацию Пользователя в УЦ Банка (с запросом на создание ему сертификата) были заведомо ложными. Ответственность в этом случае лежит на Стороне, присоединившейся к Регламенту и предоставившей данные сведения.

5.7. Возмещение убытков не освобождает Стороны от выполнения своих обязательств.

5.8. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется нормативными документами Банка и действующим законодательством Российской Федерации.

## **6. РАЗРЕШЕНИЕ СПОРОВ И КОНФЛИКТНЫХ СИТУАЦИЙ**

6.1. Сторонами в споре, в случае его возникновения, считаются Банк, являющийся владельцем УЦ Банка, и Пользователь УЦ Банка.

6.2. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

6.3. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться нормативными документами Банка и действующим законодательством Российской Федерации.

6.4. В случае возникновения конфликтной ситуации между участниками СЭД Банка при использовании СКЗИ, такая ситуация подлежит разрешению в порядке, установленном договором на обслуживание в СЭД Банка.

6.6. УЦ Банка производит проверку электронной подписи документа в случае возникновения конфликтных ситуаций, с использованием специальной утилиты «Арбитражная процедура» предназначенной для проверки соответствия электронной подписи содержанию электронного документа и определения участника СЭД.

## **Приложения:**

Приложение №1 «Руководство пользователя УЦ Банка».

Приложение №2 «Заявление на аннулирование сертификата ключа ЭП Пользователя УЦ Банка».

Приложение №3 «Заявление на приостановление действия ключа ЭП Пользователя УЦ Банка».

Приложение №4 «Заявление на возобновление действия ключа ЭП Пользователя УЦ Банка».

Приложение №5 «Заявление на подтверждение подлинности ключа ЭП Пользователя УЦ Банка».

Приложение №6 «Акт о выполненной проверке по подтверждению подлинности ЭП в электронном документе».

Приложение №7 «СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА  
В СИСТЕМЕ "iBank 2"