ПРИЛОЖЕНИЕ № 7
к Договору на обслуживание клиентов в Системе Интернет-Банк
(редакция 5.0)

РЕГЛАМЕНТ БАНКОВСКОГО ОБСЛУЖИВАНИЯ С ПРИМЕНЕНИЕМ СИСТЕМЫ ИНТЕРНЕТ-БАНК

1. ВВЕДЕНИЕ.

1.1. Система Интернет-Банк предназначена для подготовки, приема-передачи по линиям связи, учета и предварительной обработки платежных и иных электронных документов Клиентов Банком. Она построена на основе технологии обмена информацией по телекоммуникационной сети, обеспечивающей конфиденциальность, надежность и достоверность передачи информации, установление подлинности отправителя, проверку целостности и авторства документа.

1.2. Настоящий документ устанавливает порядок подключения Клиента к Системе Интернет-Банк и регламентирует передачу и обработку видов сообщений, указанных в Приложении № 5 к настоящему Договору.

1.3. При работе в Системе Клиент обязан руководствоваться Договором, данным Регламентом и Кратким руководством пользователя Системы дистанционного банковского обслуживания «iBank 2» (Интернет-Банк) АО КБ «Соколовский» (именуемым далее – Руководство), размещенном на сайте Банка. Руководство является составной частью настоящего Договора. В случае противоречий между Описанием и Договором применяются нормы последнего.

1.4. Для пользования Системой Клиент должен иметь компьютер, подключённый к Глобальной сети Internet , минимальные требования к которому указаны в разделе Требования Руководства.

2. ОБЩИЕ ПОЛОЖЕНИЯ.

2.1. Система позволяет Клиенту вводить, редактировать, удалять, подписывать и отправлять в Банк ЭД, перечисленные в Приложении № 5 к настоящему Договору, а также по согласованию Сторон просматривать информацию о состоянии своих счетов в Банке и получать выписки по счетам в электронном виде.

2.2. Электронные платежные документы, применяемые в Системе Интернет-Банк, эквивалентны бумажным платежным документам, используемым в соответствии с нормативными актами Центрального банка Российской Федерации, и являются основанием для осуществления операции по счету Клиента.

2.3. Стороны признают, что:

- используемые в Системе Интернет-Банк системы защиты информации (системы разграничения доступа, средства контроля целостности передаваемой информации, средства криптографической защиты и т.д.), механизмы доставки/приема, обработки и хранения электронных сообщений являются достаточными для обеспечения надежной и эффективной работы Системы Интернет-Банк, подтверждения авторства и подлинности информации, содержащейся в получаемых электронных документах, а также для защиты информации, циркулирующей внутри Системы, от несанкционированного доступа. Для расшифровки электронного документа и экспертной проверки электронной подписи под ним в Системе Интернет-Банк используется программное обеспечение, реализующее и использующее сертифицированные средства криптографической защиты информации (СКЗИ).

- Банк не гарантирует невозможность несанкционированного доступа к Системе третьими лицами, а Клиент принимает на себя соответствующие риски;

- если после заверения ЭД электронной подписью этот ЭД был изменён, то эта ЭП становится некорректной, то есть её проверка даёт отрицательный результат;

- подделка ЭП, то есть создание корректной ЭП ЭД, направленного Клиентом, невозможна без знания ключа ЭП и пароля;

При обмене информацией для ее шифрования используется защищенный протокол (IBTP).

2.4. ЭД/ЭПД порождает обязательства Сторон по настоящему Договору, если он инициирующей Стороной должным образом оформлен (документ содержит все реквизиты платежного (расчетного) документа, установленные банковскими правилами), ЭП под документом является подлинной и

действующей и содержит необходимое количество подписей, передан на обработку, а принимающей Стороной принят на обработку. Свидетельством того, что ЭД/ЭПД принят Банком на обработку, является значение «Доставлен» в строке статуса соответствующего документа в Системе Интернет-Банк.

2.5. Готовность Сторон к работе по Системе Интернет-Банк оформляется заполнением Сторонами Акта приема-передачи выполненных услуг по форме Приложения № 9 к настоящему Договору, а также подписанием Сторонами Сертификата ключа проверки ЭП представителя Клиента в Системе Интернет-Банк, по форме Приложения № 4 к настоящему Договору.

2.6. Банк оставляет за собой право использовать записи и данные журналов событий и аудита средств защиты, установленных, как в контуре Системы Интернет-Банк, так и вне её предела, а также документов, направленных Клиентом по Системе Интернет-Банк для доказательного разрешения споров, возникших в рамках данного Договора.

2.7. В зависимости от выбора Клиента, ключ ЭП записывается и хранится Системой на ключевом носителе (USB – накопитель или магнитный диск) или записывается и неизвлекаемо хранится в защищенной памяти USB-токена (персонального аппаратного криптопровайдера (ПАКа)). Ключи ЭП используются уполномоченными лицами Клиента в целях просмотра, подготовки и подписи ЭД/ЭПД, подготовленных с помощью Системы Интернет-Банк.

2.8. Ключ проверки ЭП после регистрации Клиента, хранится Банком в базе данных Системы Интернет-Банк.

2.9. Архив входящих и исходящих ЭД хранится Банком в базе данных Системы Интернет-Банк.

2.10. Проверка подлинности ЭП под ЭД осуществляется в автоматическом режиме программными средствами Системы Интернет-Банк.

3. ОБЯЗАННОСТИ СТОРОН.

3.1. В рамках настоящего Регламента Банк обязуется:

3.1.1. Принимать от Клиента на условиях настоящего Договора по электронным каналам связи должным образом оформленные электронные документы с контролем их целостности и авторства.

3.1.2. Осуществлять обработку ЭД только с подлинной ЭП лиц, идентификатор ключа проверки ЭП которых соответствует данным, указанным в Сертификате ключа проверки ЭП.

3.1.3. Осуществлять обработку и исполнение полученных ЭД Клиента в строгом соответствии с установленными законодательством РФ и нормативными актами Банка России нормами, техническими требованиями и инструкциями.

3.1.4. Предоставлять Клиенту информацию о результатах проверки и обработки принятого ЭД Клиента или отказе в приеме на обработку с указанием причин.

3.1.5. По результатам обработки и исполнения ЭД Клиента, а также по мере совершения иных операций по счету, не позднее следующего рабочего дня после совершения операции, подготавливать и предоставлять Клиенту в ответ на его запрос выписки по счету (счетам) с указанием основных реквизитов платежного документа, на основании которого совершена операция по счету.

3.1.6. Своевременно информировать Клиента об изменениях порядка осуществления обработки ЭД и другой информации посредством направления ЭСИД по Системе Интернет-Банк. Оказывать консультационные услуги Клиенту по вопросам технической и организационной поддержки в рамках оказания услуг с использованием Системы Интернет-Банк, а также информировать и оказывать консультационные услуги Клиенту по вопросам информационной безопасности при работе в Системе Интернет-Банк.

3.1.7. Осуществлять необходимую модернизацию программного обеспечения Системы Интернет-Банк.

3.1.8. Сообщать Клиенту о непредвиденных сбоях в работе Системы Интернет-Банк для принятия им мер по своевременной доставке бумажного документа в Банк.

3.2. В рамках данного Регламента Клиент обязуется:

3.2.1. Инициировать соединение с Банком по Системе Интернет-Банк для получения/передачи ЭД в Банк/из Банка.

3.2.2. Ознакомиться с инструкциями по работе в Системе Интернет-Банк, размещенными на сайте Банка и руководствоваться их требованиями и положениями при работе в Системе Интернет-Банк.

3.2.3. Осуществлять ввод документов (и осуществлять контроль введенной информации) в электронном виде, соблюдая порядок подготовки документов, обеспечивая заполнение форм в соответствии с банковскими требованиями и законодательством РФ.

3.2.4. Осуществлять в течение любого рабочего дня не менее одного сеанса связи с Банком для получения выписок по счету(ам), контролю проводимых операций, а также возможных экстренных (технических) или информационных сообщений Банка, либо другой актуальной информации.

3.2.5. Выполнять требования по оформлению и защите передаваемой информации в виде ЭД, защите ключей ЭП, носителей ключевой информации, паролей доступа и другой информации, передаваемой и получаемой по Системе Интернет-Банк.

3.2.6. Соблюдать порядок осуществления приема и передачи ЭД и обеспечивать передачу только надлежащим образом оформленных документов.

3.2.7. Самостоятельно и за свой счет обеспечивать режим информационной безопасности при работе в Системе Интернет-Банк путем принятия соответствующих организационно-технических мер, в том числе описанных в настоящем Договоре, на сайте Банка и/или в сообщениях, рассылаемых Клиенту по каналам Системы Интернет-Банк.

3.2.8. По запросу Банка подтвердить выполнение мероприятий по защите от воздействия вредоносных программ, в том числе вредоносного кода, либо сообщить о невыполнении таких мероприятий или выполнении их не в полном объеме. Подтверждение Клиент направляет в той же форме, что и полученный от Банка запрос.

3.3. В рамках данного Регламента Стороны взаимно обязуются:

3.3.1. Не осуществлять действий, наносящих ущерб другой Стороне вследствие использования Системы Интернет-Банк.

3.3.2. Не осуществлять операцию по ЭД, заверенному ЭП, если программа проверки, используя действующий ключ проверки подписывающей Стороны, не подтвердила подлинность ЭП подписывающей Стороны под ЭД.

3.3.3. При осуществлении операций на основании полученных по Системе ЭД руководствоваться требованиями законодательства РФ, нормативных актов Банка России, и соглашений (договоров), заключенных между Банком и Клиентом.

3.3.4. Обеспечивать целостность и сохранность программных средств, ЭД, ключевой информации, ключевых носителей, паролей доступа, а также иной информации, передаваемой и получаемой по Системе Интернет-Банк.

3.3.5. Вести архивы передаваемых и получаемых по системе Интернет-Банк документов на магнитных и бумажных носителях, хранить их в соответствии с порядком и сроками, установленными для хранения данного вида документов.

4. УСЛОВИЯ И ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ.

4.1. Общие положения

4.1.1. Программное обеспечение Банка настроено на взаимодействие с Системой Интернет-Банк, разработанной ООО «БИФИТ», права на которую принадлежат АО «БИФИТ», и предполагает использование Клиентом этой же Системы.

4.1.2. Банк и Клиент взаимно признают достаточную криптографическую устойчивость используемых в Системе Интернет-Банк алгоритмов, используемых для создания ключа ЭП.

4.1.3. Стороны взаимно признают достоверность и достаточную защищенность от подделок ЭП, созданной посредством Системы Интернет-Банк, на ЭД, передаваемых согласно условиям настоящего Договора.

4.1.4. После заполнения Клиентом Заявления (Приложение № 1 к настоящему Договору) и оплаты вознаграждения Банка за выбранные в рамках Договора услуги Стороны проводят техническую и организационную подготовку по подключению Клиента к Системе Интернет-Банк и регистрации ключей ЭП Клиента в порядке, определенном настоящим Регламентом и Руководством. По результатам успешного исполнения указанных процедур Сторонами должны быть подписаны Акт приема-передачи выполненных услуг (Приложение № 9 к настоящему Договору) и Сертификат ключа проверки ЭП представителя Клиента в Системе Интернет-Банк (Приложение № 4 к настоящему Договору).

4.1.5. Подготавливаемые в Системе Интернет-Банк ЭД проходят автоматическую проверку на датировку, присутствие обязательной информации в полях документа, на соответствие вводимых данных - реквизитам, записанным во встроенных справочниках и иное в соответствии с принятой технологией Системы Интернет-Банк.

4.1.6. Для повышения безопасности на стороне Банка используется механизм запроса дополнительного подтверждения при входе в Систему Интернет-Банк одноразовым паролем. Клиент получает от Банка сообщение в формате SMS-сообщения на сотовый (мобильный) телефон, работающий в стандарте GSM и имеющий техническую возможность приема сообщений формата SMS (Short Messaging Service) принадлежащий Клиенту или доверенному лицу Клиента. Номера телефонов Клиента, используемые для получения SMS-сообщений, указываются в Заявлении о присоединении или в Заявлении об информировании. Уведомление отправляется на номер телефона сотрудника Клиента, чьим ключом ЭП был выполнен вход в Систему.

4.1.7. После заполнения электронной формы платежного или иного документа Клиента осуществляется его подписание. Клиент подписывает ЭПД своей ЭП, на основании которой однозначно

устанавливается авторство документа. Количество подписей под ЭПД должно соответствовать количеству подписей, указанных в карточке с образцами подписей и оттиска печати Клиента и Соглашении о подписании распоряжений по счету лицами, наделенными правом подписи, хранящихся в Банке.

4.1.8. В целях усиления мер по обеспечению информационной безопасности и минимизации рисков исполнения Банком несанкционированных Клиентом переводов по Системе после отправке ЭПД в Банк Клиент получает от Банка SMS-сообщение, содержащее в себе одноразовый пароль для подтверждения ЭПД (пакета ЭПД) о переводе денежных средств направленного/ных Банку для исполнения, сумму перевода (переводов), номер платежного поручения (в случае подтверждения одного ЭПД), информацию о получателе средств (в случае подтверждения одного ЭПД), либо общее количество документов (для подтверждения нескольких ЭПД).

4.1.9. Для подтверждения исполнения ЭПД Банком, Клиент проверяет сумму и реквизиты ЭПД, полученные в SMS-сообщении, и в случае согласия вводит полученный одноразовый пароль в соответствующем поле Системы Интернет-Банк.

4.1.10. В случае несогласия с реквизитами ЭПД, полученными в SMS-сообщении, Клиент не подтверждает одноразовым паролем ЭД и в обязательном порядке уведомляет Банк о появлении несанкционированного ЭД.

4.1.7. На этапе обработки ЭД в Банке осуществляется автоматический контроль (на соответствие электронной подписи содержимому документа, на соответствие количества подписей, на целостность и достоверность ЭП, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка и банка получателя, установленных Банком России, и иное в соответствии с принятой технологией). В случае выявления несоответствий в ходе автоматической проверки документа, операции по документу не проводятся, а Клиент получает информацию с указанием причин отказа в приеме на обработку ЭД, а в строке статуса ЭД в соответствующем модуле устанавливается значение «Отвергнут».

4.1.8. Основанием для отказа Банка от приема и/или исполнения ЭД служат:

- отрицательный результат автоматической проверки ЭП на ЭД;
- отрицательный результат контроля целостности ЭД,
- отрицательный результат структурного контроля ЭД,
- дублирование ЭД,
- несоответствие операции режиму работы Счета,
- отсутствие или недостаток денежных средств для проведения операций на счете Клиента; если прием к исполнению в этом случае не предусмотрен законодательством или договором,
- несоответствие количества подписей, которыми подписан ЭД, количеству, указанному в карточке с образцами подписей и оттиска печати Клиента и Соглашении о подписании распоряжений по счету лицами, наделенными правом подписи;
- контроль операций на предмет соответствия требованиям законодательству Российской Федерации, в том числе требованиям Федерального закона от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»,
- отрицательный результат контроля значений реквизитов ЭД, их допустимости и соответствия требованиям нормативных документов Банка России, ФНС и Банка.
- отрицательный результат контроля наличия согласия третьего лица на распоряжение денежными средствами при приеме к исполнению распоряжения Клиента, требующего такого согласия в соответствии с федеральным законом, договором,
- отрицательный результат контроля выполнения условий перевода.

В случае отказа Банком в приеме ЭД к исполнению, Банк направляет Клиенту информацию об аннулировании документа с указанием причины, по которой документ не будет исполнен Банком, даты аннулирования, в строке статуса ЭД устанавливается значение «Отвергнут».

Клиент может отозвать принятый Банком платежный документ до наступления безотзывности перевода, направив Банку средствами Системы заявление об отзыве (Отзыв) с указанием реквизитов отзываемого документа.

Безотзывность перевода денежных средств по ЭПД наступает в соответствии с Федеральным законом №161-ФЗ.

До наступления безотзывности перевода денежных средств по ЭПД на основании поступившего заявления об отзыве (Отзыва) ЭПД Банком не исполняется, указывается причина неисполнения - «отзыв», а в строке статуса ЭПД устанавливается значение «Отвергнут».

При положительном результате процедур приема к исполнению Банк принимает ЭПД к исполнению и направляет Клиенту информацию, позволяющую Клиенту идентифицировать ЭПД и дату

приема его к исполнению, при этом в Системе Интернет-Банк ЭД присваивается статус «На исполнении».

В случае помещения ЭПД в очередь не исполненных в срок распоряжений в ЭПД и в уведомлении в электронном виде, направляемом с использованием Системы, Банк указывает дату помещения распоряжения в очередь, ЭПД в Системе Интернет-Банк присваивается статус «В картотеке».

Банк информирует Клиента о каждой операции, совершенной с использованием Системы Интернет-Банк, посредством направления Клиенту ежедневной (промежуточной, окончательной) выписки по соответствующему Счету в электронном виде по Системе Интернет-Банк и исполненного ЭПД с указанием даты его исполнения.

Выписки становятся доступны Клиенту в Системе Интернет-Банк с момента их отправки.

В случае если Банк выступает в качестве банка плательщика уведомление в электронном виде о списании денежных средств со Счета плательщика осуществляется также путем присвоения Банком ЭПД Клиента в системе Интернет-Банк статуса, подтверждающего исполнение «Исполнен».

4.1.9. Активной стороной при установлении связи является Клиент.

4.2. Сроки обработки документов.

4.2.1. Система Интернет-Банк функционирует ежедневно с 00.00 часов до 24.00 часов.

Прием к исполнению ЭПД Клиента производится Банком по рабочим дням в соответствии с заключенными с Клиентом Договорами банковского счета и Графиком обслуживания Клиентов, установленным Банком.

4.2.2. Стороны признают в качестве единой шкалы времени при направлении ЭД по Системе Интернет-Банк московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4.3. Аварийный режим работы.

4.3.1. При возникновении неисправности технических или программных средств Клиента, или других нештатных ситуаций, возникающих не со стороны и не по вине Банка, делающих невозможным передачу ЭД Клиента Банку по Системе Интернет-Банк, Клиент в тот же день должен предупредить уполномоченных сотрудников Банка, и осуществить действия для доставки в Банк уполномоченным лицом надлежащим образом оформленных документов на бумажных носителях в соответствии с Графиком обслуживания Клиентов, установленным Банком.

5. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА.

5.1. ОБЩИЕ ПОЛОЖЕНИЯ.

5.1.1. Защита информации в Системе Интернет-Банк является многоуровневой и задействует возможности операционной системы, прикладного программного обеспечения, специализированных программных и технических средств и организационных мер (наличие соответствующих администраторов), организации хранения ПО, используемого в Системе Интернет-Банк.

5.1.2. Система комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание (генерация) ключей/ключей проверки шифрования и ЭП;
- ЭП под ЭД;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- проверка корректности ЭП;
- подтверждение авторства и целостности электронных документов;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- доказательную базу, применяемую при разборе конфликтных ситуаций.

5.1.3. Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД подписанных ЭП, а также архивы ключей проверки ЭП. Хранение контрольных архивов осуществляется в течение трех лет с момента проведения операций.

5.1.4. При проверке подписи под документом используется соответствующий действующий ключ проверки ЭП Клиента, подписавшего ЭД.

5.1.5. Обработка принятых Банком от Клиента ЭД производится только при условии корректности ЭП на ЭД.

5.2. ПОРЯДОК ГЕНЕРАЦИИ И РЕГИСТРАЦИИ КЛЮЧЕЙ ЭП.

5.2.1. В процессе предварительной регистрации Клиент самостоятельно создает ключ ЭП и парный ему ключ проверки ЭП. Ключ ЭП Клиента сохраняется на ключевом носителе Клиента (дискете/USB-

флеш-накопителе или на ПАКе) в Хранилище ключей. Ключ проверки ЭП по защищенному соединению передается в Банк и предварительно регистрируется в Системе Интернет-Банк. Также ключ проверки ЭП должен быть распечатан Клиентом на бумажном носителе в виде Сертификата ключа проверки ЭП в двух экземплярах. Форма Сертификата приведена в Приложении № 4 к настоящему Договору. Оба экземпляра Сертификата должны быть подписаны собственноручными подписями уполномоченных лиц Клиента согласно карточке с образцами подписей и оттиска печати Клиента и Соглашения о подписании распоряжений по счету лицами, наделенными правом подписи, хранящихся в Банке и представлены в Банк для регистрации согласно п.5.2.5 настоящего Регламента.

В Сертификате (Приложение № 4 к Договору) на владельца ключа ЭП, которому на основании доверенности от Клиента предоставлено только право просмотра и создания ЭД, ЭПД и ЭСИД без права их подписи и отправки в Банк, в пункте 10 «Примечания» указывается *"БЕЗ ПРАВА ПОДПИСИ ЭПД"*

5.2.2. Все ключи ЭП в процессе генерации защищаются паролями. Указанный пароль является конфиденциальной информацией владельца ключа. Владелец ключа несет ответственность за обеспечение сохранности такой конфиденциальной информации.

5.2.3. Владельцы ключей ЭП, созданных в Системе Интернет-Банк, несут персональную ответственность за обеспечение сохранности ключевой информации, защиты ключевых файлов (элементов) и ключевых носителей от несанкционированного доступа.

5.2.4. Все процедуры окончательной регистрации и проверки ключей проверки ЭП, происходят только в помещениях Банка и только на программном обеспечении и оборудовании Банка.

5.2.5. При регистрации ключа проверки ЭП Клиента в Банке производится сверка ключа проверки ЭП Клиента с ключом проверки ЭП, напечатанным в Сертификате ключа проверки ЭП, и проверка лиц, на имя которых сформированы ключи, на соответствие их с именами, фамилиями, отчествами (при наличии) и образцами подписей и оттиском печати, указанными в банковской карточке Клиента, Соглашении о подписании распоряжений по счету лицами, наделенными правом подписи, доверенностями, хранящимися в Банке.

5.2.6. Ключ ЭП Клиента регистрируется только после получения Банком надлежаще оформленного и заверенного Клиентом Сертификата ключа проверки ЭП, а также успешной верификации данных, указанных в п.п.5.2.5 настоящего Регламента. При регистрации ключа Клиента в Системе Интернет-Банк уполномоченные на совершение соответствующих действий сотрудники Банка проставляют в Сертификате ключа проверки ЭП отметки о дате регистрации и сроке его действия в Системе Интернет-Банки заверяют печатью Банка. После регистрации ключа ЭП Клиента в Системе, один экземпляр Сертификата ключа проверки ЭП на бумажном носителе передается Клиенту, второй - остается на хранении в Банке, а его электронный аналог находится в каталоге ключей Банка и Клиента.

5.3. ПОРЯДОК ХРАНЕНИЯ И СМЕНЫ КЛЮЧЕЙ ЭП.

5.3.1. ПОРЯДОК ХРАНЕНИЯ КЛЮЧЕЙ.

5.3.1.1. Надежность средств криптозащиты и подлинность передаваемой по каналам связи информации обеспечивается только при условии сохранности от компрометации действующих ключей ЭП. К событиям, связанным с компрометацией или подозрением на компрометацию ключа относятся, включая, но не ограничиваясь, следующие события:

- утеря носителя ключевой информации, в том числе с последующим обнаружением;
- выход из строя носителя ключевой информации, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- обнаружение факта или угрозы использования (копирования) паролей доступа и/или доступа к Системе Интернет-Банк неуполномоченных лиц (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Системы Интернет-Банк, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение вредоносных программ, в том числе вредоносного кода, в компьютере, используемом для работы в Системе Интернет-Банк.

5.3.1.2. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить условия хранения своих ключей ЭП, исключающие возможность их компрометации. В случае любого подозрения в компрометации ключей ЭП Клиент обязан немедленно оповестить Банк о необходимости блокировки ключей ЭП Клиента в соответствии с Соглашением о порядке информирования при работе в Системе Интернет-Банк (Приложение № 10 к Договору). Допускается возможность дистанционного оповещения уполномоченного сотрудника Банка о необходимости блокировки ключей ЭП Клиента с указанием Кодового слова, с последующим обязательным предоставлением в Банк на бумажном носителе письменного заявления о блокировке ключей ЭП по форме Приложения № 12 к настоящему Договору.

5.3.1.3. Банк не несет ответственности в случаях компрометации действующих ключей ЭП Клиента за последствия, которые могут возникнуть в результате данной компрометации. При рассмотрении Банком ЭД считается действительным и подлинным, если он подписан подлинной ЭП Клиента, сформированной при использовании действующего ключа ЭП, сгенерированного Клиентом в процессе создания ключей ЭП, и зарегистрированного в Системе Интернет-Банк на основании Сертификата ключа проверки ЭП, предоставляемого Клиентом в Банк.

5.3.1.4. Выведенные из употребления ключи хранятся в Банке те же сроки, что и документы, подписанные и зашифрованные этими ключами, т.е. в соответствии с правилами организации государственного архивного дела, но не менее пяти лет.

5.3.2. ПОРЯДОК СМЕНЫ КЛЮЧЕЙ ЭП.

5.3.2.1. Смена ключей производится при:

1. истечении срока действия ключей;
2. компрометации ключей;
3. переходе от обычных ключевых носителей к ПАКам.
4. смены наименования Клиента.

5.3.2.2. Срок действия ключей ЭП составляет 24 месяца (срок действия ключа ЭП исчисляется с даты регистрации Сертификата ключа проверки ЭП в Банке уполномоченным сотрудника Банка).

5.3.2.3. Смена ключей уполномоченных лиц Клиента производится в соответствии с п.5.2. данного Регламента.

5.3.2.4. ЭД, подписанный ЭП Клиента, сформированной с использованием новых ключей, принимается Банком только после регистрации новых ключей ЭП Клиента в соответствии с порядком, изложенным в п.5.2 данного Регламента.

5.4. ПОРЯДОК БЛОКИРОВКИ КЛЮЧЕЙ ЭП.

5.4.1. Банк блокирует (приостанавливает) действие ключа с момента получения уполномоченными службами Банка на бумажном носителе письменного заявления Клиента о блокировке ключа, содержащего причину блокировки, ФИО владельца и/или ID ключа, указанного в Сертификате ключа проверки ЭП, составленного по форме Приложения № 12 к настоящему Договору, подписанного лицами, наделенными правом подписи согласно банковской карточке Клиента и Соглашения о подписании распоряжений по счету, в соответствии с Соглашением о порядке информирования при работе в Системе Интернет-Банк (Приложение № 10 к настоящему Договору).

5.4.2. В экстренных случаях блокировка может быть произведена при уведомлении Банка по телефону на основании Кодового слова в соответствии с Соглашением о порядке информирования при работе в Системе Интернет-Банк (Приложение № 10 к настоящему Договору).

При использовании средств коммуникации, указанных в настоящем пункте, Клиент обязуется не позднее 3-х (Трех) рабочих дней со дня направления извещения/уведомления по телефону, представить в Банк подтверждающее письменное заявление, составленного по форме Приложения № 12 к настоящему Договору. После блокирования ключа, прием и обработка документов, подписанных данным ключом, прекращаются.

5.4.3. Банк может блокировать ключ Клиента самостоятельно в случае возникновения подозрений в компрометации ключа ЭП. В этом случае уполномоченный сотрудник Банка в течение 1 (Одного) рабочего дня со дня принятия такого решения извещает Клиента о принятом решении и о приостановлении обработки ЭД, подписанных этим ключом в соответствии с Соглашением о порядке информирования при работе в Системе Интернет-Банк (Приложение № 10 к Договору).

5.4.4. Снятие блокировки производится на основании письменного заявления Клиента об устранении причин, приведших к блокированию ключа, и составленного в произвольной форме и подписанного лицами, наделенными правом подписи согласно банковской карточке Клиента и Соглашения о подписании распоряжений по счету. В случае блокировки ключа по инициативе Банка снятие блокировки с ключа Клиента производится по согласованию с Клиентом, но после получения его письменного разрешения.

5.5. ПОРЯДОК ИСКЛЮЧЕНИЯ ЭП.

5.5.1. Банк исключает ключ из каталога (базы) действующих ключей, с момента получения уполномоченными службами Банка письменного заявления Клиента, составленного по форме Приложения № 12 к Договору и подписанного уполномоченными лицами Клиента согласно банковской карточке с образцами подписей и оттиска печати и Соглашению о подписании распоряжений по счету лицами, наделенными правом подписи. Ключ ЭП Клиента исключается из каталога действующих ключей, прием и обработка ЭД, подписанных таким ключом, прекращается.

5.5.2. Ключи ЭП Клиента, срок действия которых истек, признаются недействующими автоматически и исключаются из каталога действующих ключей в Системе Интернет-Банк. Вход в

Систему, так же как и другие операции с использованием просроченного ключа ЭП становятся невозможными. Банк не несет ответственность за несвоевременную смену Клиентом ключей ЭП и возникшие в связи с этим последствия для Клиента.

5.5.3. Банк и Клиент обеспечивают сохранность исключенных ключей ЭП Клиента согласно п.п.5.3.1. данного Регламента, при этом исключенные ключи хранятся те же сроки, что и документы, подписанные и зашифрованные этими ключами.

5.6. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭП.

5.6.1. В случае компрометации или подозрения на компрометацию ключа Клиент должен незамедлительно известить уполномоченных сотрудников Банка для блокировки соответствующего ключа, в соответствии с порядком, установленным п.5.4. данного Регламента и Соглашением о порядке информирования при работе в Системе Интернет-Банк(Приложение № 10 к настоящему Договору).

5.6.2. В случае не подтверждения компрометации ключа, Банк производит снятие блокировки ключа в соответствии с п.5.4.4 данного Регламента.

5.6.3. В случае подтверждения компрометации ключа Банк исключает скомпрометированный ключ в соответствии с п.5.5 данного Регламента.

5.6.4. ЭД, подписанные скомпрометированным ключом, и соответствующий ему ключ проверки ЭП Клиента, хранятся в соответствии с правилами организации государственного архивного дела, но не менее пяти лет.

5.7 ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ АППАРАТНЫХ КРИПТОПРОВАЙДЕРОВ

5.7.1 Для обеспечения безопасного хранение ключей ЭП во встроенной защищенной памяти без возможности их экспорта Банк передает в пользование Клиенту USB-токены (персональные аппаратные криптопровайдеры (ПАКи)).

5.7.2. Перечень, предоставляемых в рамках настоящего Регламента ПАКов определен в разделе Поддерживаемые аппаратные устройства «Краткого руководства пользователя системы дистанционного банковского обслуживания «iBank 2» (Интернет-Банк) АО КБ «Соколовский».

5.7.3. Передача ПАКов осуществляется на основании Заявления о присоединении по форме Приложения № 1 к договору (при первичном обращении) или Заявления на подключение услуг в Системе Интернет-Банк по форме Приложения № 6 к Договору (при обращении в рамках действующего Договора). При оформлении заявления Клиент указывает количество ПАКов, необходимых Клиенту. Банк рекомендует Клиентам для каждого лица, наделенного ЭП, использовать отдельный ПАК.

5.7.4. Передача ПАКов осуществляется путем подписания Сторонами Акта приема-передачи программного обеспечения и средств криптографической защиты информации (Приложение № 3 к настоящему Договору), которым подтверждается передача Клиенту заявленного количества ПАКов, пользовательской документации и драйверов для работы ПАКов.

5.7.5. За предоставленные материалы по защите ключей ЭП Клиента с использованием ПАКа Клиент осуществляет оплату комиссионного вознаграждения в соответствии с действующими Тарифами Банка.

5.7.6. Для активации и начала использования ПАКа в Системе Интернет-Банк Клиент обязан осуществить генерацию/смену ключей ЭП в порядке, указанном в разделе 5.2. Регламента, с использованием в качестве ключевого носителя ПАКа.

5.7.7. За первичную регистрацию ключей ЭП с использованием ПАК при подключении Клиентом услуги по защите ключей ЭП, за плановую и внеплановую смену ключей ЭП взимается комиссия в соответствии с действующими тарифами Банка, за исключением случая указанного в п. 5.7.8. Регламента.

5.7.8. Клиент вправе в период гарантийного срока заменить неисправное устройство без внесения дополнительной платы. Срок замены неисправного устройства составляет не более трех рабочих дней. Гарантийный срок составляет 12 месяцев со дня передачи ПАКа Клиенту, и не распространяется на устройства с видимыми повреждениями, произошедшими в результате внешних воздействий на устройство.

5.7.8. В случае утраты устройства, Клиент обязан незамедлительно обратиться в Банк для блокировки ключей ЭП, сохраненных на утраченном ПАКе в порядке, установленном Соглашением о порядке информирования при работе в Системе Интернет-Банк (Приложение № 10 к настоящему Договору), при этом Клиент предоставляет заявления по форме Приложения № 12 и Приложения № 6 к настоящему Договору.