«Республиканский Кредитный Альянс» ООО

Коммерческий Банк

УТВЕРЖДЕНО
Правлением
Коммерческого Банка
«Республиканский Кредитный Альянс»
(общество с ограниченной ответственностью)
Протокол № 25-07/2024 от 25.07.2024

Председатель Правления
_____И.В. Карлинский

РЕГЛАМЕНТ

обслуживания корпоративных клиентов с использованием системы дистанционного обслуживания «iBank2»
в Коммерческом Банке «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью)

(новая редакция)

г. Москва, 2024

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АБС - автоматизированная банковская система, используемая Банком.

Автоматизированное рабочее место Клиента (АРМ Клиента) - аппаратно-программные средства, средства вычислительной техники, используемые Клиентом для работы с Системой ДБО «iBank2» в рамках настоящего Регламента.

Авторизация - разрешение Банка на вход в Систему ДБО «iBank2» или на проведение Операции после удостоверения права осуществления Клиентом действий в Системе ДБО «iBank».

Аннулирование СКП ЭП - процедура, при которой действие СКП ЭП Клиента полностью прекращается до истечения срока его действия и возобновлению не подлежит. В рамках Системы ДБО «iBank2» аннулирование обеспечивается удалением СКП ЭП из списка СКП ЭП Клиента.

Аутентификация - выполняемая средствами Системы ДБО «iBank2» процедура проверки подлинности и принадлежности Клиенту введенного им имени пользователя (задействованного ключа ЭП) и пароля в Системе ДБО «iBank2». Банком обеспечивается аутентификация входящих электронных документов и взаимная (двусторонняя) аутентификация Банка и Клиента.

Банк – Коммерческий Банк «Республиканский Кредитный Альянс» ООО.

Банковский счет - счет, открытый Клиенту на основании договора банковского счета в валюте Российской Федерации или иностранной валюте для осуществления операций, разрешенных действующим законодательством Российской Федерации.

Владелец СКП ЭП - лицо, которому в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» выдан сертификат ключа проверки электронной подписи. В целях настоящего Регламента под Владельцем СКП ЭП понимается физическое лицо - представитель Клиента, Ключ проверки ЭП которого зарегистрирован в Системе ДБО «iBank2» в соответствии с настоящим Регламентом.

Вредоносный код - компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Сторон Договора, приводящая к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Договор банковского счета - соглашение между Банком и Клиентом, составленное в соответствии с действующим законодательством Российской Федерации, на основе которого Банк обязуется принимать и зачислять поступающие на банковский счет, открытый Клиенту (владельцу банковского счета), денежные средства, выполнять распоряжения Клиента о перечислении и выдаче соответствующих сумм с банковского счета и проведении других операций по банковскому счету.

Договор дистанционного банковского обслуживания с использованием Системы ДБО «iBank2» (Договор) - договор между Банком и Клиентом об использовании Системы ДБО «iBank2», заключенный в порядке, установленном настоящим Регламентом, и включающий в качестве составных и неотъемлемых частей Тарифы по обслуживанию в Системе ДБО «iBank2» (далее - Тарифы).

Защита информации - комплекс организационно-технических мероприятий, проводимых Банком с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации в Системе ДБО «iBank2».

Информационная безопасность - состояние защищенности информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п., состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Клиент (корпоративный клиент) - юридическое лицо, индивидуальный предприниматель, находящиеся на обслуживании в Банке и имеющее открытый Банковский счет.

Ключ проверки ЭП - (открытый ключ) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи). В целях настоящего Регламента Ключ проверки ЭП - ключ (последовательность байт), зависящий от Ключа ЭП Клиента, самостоятельно формируемый Клиентом с использованием средств СКЗИ в Системе ДБО «iBank2» и предназначенный для проверки Банком подлинности ЭП в электронном документе, сформированном Клиентом. Ключ проверки ЭП указывается в СКП ЭП.

Ключ ЭП - (закрытый ключ) - уникальная последовательность символов, предназначенная для создания электронной подписи. В целях настоящего Регламента Ключ ЭП - ключ (последовательность байт), самостоятельно формируемый Клиентом с использованием программных средств Системы ДБО «iBank2» и предназначенный для авторизации в Системе ДБО «iBank2» и формирования Клиентом электронной подписи в документах.

Ключевой носитель - устройство (токен), позволяющее генерировать Ключи ЭП внутри себя, обеспечивать их защищенное неизвлекаемое хранение и формировать ЭП под электронными документами внутри устройства.

Компрометация Ключа ЭП (нарушение конфиденциальности Ключа ЭП) - констатация обстоятельств, при которых возможно несанкционированное использование Ключа ЭП неуполномоченными лицами и/или произошла утрата доверия к тому, что используемый Ключ ЭП обеспечивает безопасность информации.

Операционное время - время, в течение которого поступившие от Клиента по Системе ДБО «iBank2» платежные документы принимаются Банком в обработку, исполняются и отражаются по счетам бухгалтерского учета. Для различных Операций, осуществляемых с использованием Системы ДБО «iBank2», Операционное время может отличаться. Информация об установленном Операционном времени указана в Тарифах.

Операция - действия, осуществляемые Банком с денежными средствами Клиента на его Банковских счетах на основании электронного документа, переданного Клиентом в Банк с использованием Системы ДБО «iBank2» в порядке, установленном настоящим Регламентом, и содержащего указание на распоряжение денежными средствами Клиента.

Платежный ЭД - распоряжения оформленные в виде электронного документа.

Перевод без добровольного согласия клиента – наличие признаков осуществления перевода денежных средств без согласия клиента, или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием.

Признаки осуществления перевода денежных средств без добровольного согласия клиента - совокупность признаков, при наличии которых Банк имеет основания заподозрить, что перевод денежных средств осуществляется без ведома и добровольного согласия Клиента. Признаки осуществления перевода денежных средств без добровольного согласия клиента устанавливаются Банком России и размещаются на его официальном сайте в информационно-телекоммуникационной сети Интернет.

Банк в рамках реализуемой им системы управления рисками определяет во внутренних документа процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без добровольного согласия клиента, на основе анализа характера, параметров и объема совершаемых его клиентами операций (осуществляемой клиентами деятельности).

Рабочий день - день, который в соответствии с законодательством Российской Федерации не является выходным и (или) нерабочим праздничным днем.

Распоряжения - распоряжения о переводе денежных средств, составляемые плательщиками, получателями средств, а также лицами, органами, имеющими право на основании закона предъявлять распоряжения к банковским счетам плательщиков, банками, в том числе платежные документы.

Регламентные работы - комплекс технических мероприятий, проводимых Банком периодически или регулярно при эксплуатации программно-аппаратного комплекса Системы ДБО «iBank2».

Сертификат ключа проверки электронной подписи (СКП ЭП) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром (уполномоченной организацией, осуществляющей функции по созданию и выдаче сертификатов ключей проверки электронных подписей), и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. В целях настоящего Регламента СКП ЭП - документ, сформированный программными средствами Системы ДБО «iBank2» при генерации Клиентом Ключа ЭП и Ключа проверки ЭП, оформленный в соответствии с требованиями настоящего Регламента. При формировании СКП ЭП в Системе ДБО «iBank» в качестве удостоверяющего центра выступает Банк.

Система дистанционного банковского обслуживания «iBank2» (Система ДБО «iBank2») - система дистанционного банковского обслуживания «Банк-Клиент «iBank», представляющая собой комплекс программно-аппаратных средств, устанавливаемых и согласовано эксплуатируемых Клиентом и Банком, обеспечивающих подготовку, защиту, передачу Клиентом в Банк ЭД, обработку Банком ЭД, формирование Банком и предоставление Клиенту выписок о движении денежных средств по банковскому счету и прочих сообщений с использованием электронно-вычислительных средств обработки информации.

Система «Fraud-мониторинг» - набор средств обнаружения фактов мошенничества реализованный на базе ядра АБС «Опердень» для выявления фальсифицированных ЭД.

Средства доступа - программно-аппаратные средства, логины, пароли, Ключевые носители, используемые для доступа к Системе ДБО «iBank2».

Средства криптографической защиты информации (СКЗИ) - совокупность программнотехнических средств, обеспечивающих применение ЭП и шифрования при организации электронного документооборота в Системе ДБО «iBank2». В качестве СКЗИ применяются аппаратные Ключевые носители, обеспечивающие генерацию Ключа ЭП Клиента по российскому криптографическому алгоритму ГОСТ Р34.10-2012 непосредственно внутри самого устройства и неизвлекаемость (невозможность считывания) закрытого Ключа ЭП Клиента.

Средства электронной подписи (Средства ЭП) - 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.

Стороны - Банк и Клиент при совместном упоминании.

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.

ЭП подтверждает авторство ЭД, созданного в Системе ДБО «iBank2», и является средством проверки неизменности его содержания, так как любое изменение ЭД после его подписания ЭП нарушает целостность ЭП.
В Системе ДБО «iBank2» используется усиленная квалифицированная электронная подпись (УКЭП).
Электронное средство платежа - средство и (или) способ, позволяющие Клиенту составлять, удостоверять и передавать Распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационнокоммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. Система ДБО «iBank2» является электронным средством платежа.
Электронный документ (ЭД) - документ, представленный в электронной форме, подписанный ЭП, подготовленный и переданный с использованием программного обеспечения Системы ДБО «iBank2» в соответствии со всеми процедурами защиты информации.
Юридическое дело - совокупность представленных Клиентом для открытия Банковского счета и формируемых в процессе обслуживания документов, позволяющих установить правоспособность Клиента, подтвердить полномочия лиц, выступающих от его имени.
БДБР о СБСК – База данных Банка России о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента.
Федеральный закон № 161-ФЗ - Федеральный закон от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент определяет условия, на которых может быть заключен Договор между Банком и Клиентом, и устанавливает порядок взаимоотношений между Сторонами при осуществлении Операций с использованием Системы ДБО «iBank2».
2.2. Все Приложения к настоящему Регламенту являются его неотъемлемой частью.
2.3. До заключения договора на обслуживание Банк обязан информировать Клиента об условиях использования Системы ДБО «iBank2», в частности о любых ограничениях, способов и мест использования, случаях повышенного риска использования Системы ДБО «iBank2».
2.4. Настоящий Регламент и иная информация в отношении использования Системы ДБО «iBank2» размещается на сайте Банка по адресу www.cbrca.ru и на информационных ресурсах в месте обслуживания Клиентов в Банке.
2.5. Клиент до заключения договора на обслуживание обязан ознакомиться с правилами, изложенными в настоящем Регламенте и иной информацией в отношении использования Системы ДБО «iBank2».
2.6. Размещение настоящего Регламента на сайте Банка и в месте обслуживания Клиентов является достаточным в целях исполнения Банком обязанности информирования Клиента об условиях использования Системы ДБО «iBank2».
2.7. Заключение Договора производится на основании Заявления (типовая форма Заявления и Договора утверждается распорядительным документом Председателя Правления. Заключая договор, Клиент подтверждает, что до заключения Договора:

- проинформирован об условиях использования системы ДБО «iBank2», об ограничениях способов, мест использования и случаях повышенного риска использования системы ДБО «iBank»;
- ознакомлен с Регламентом и Тарифами, согласен и обязуется их неукоснительно соблюдать их требования.

2.8. Заявление подается Клиентом в Банк на бумажном носителе.
2.9. Договор вступает в силу с даты его подписания.

2.10. Обслуживание Клиента с использованием Системы ДБО «iBank2» начинается с даты окончательной регистрации Клиента в Системе ДБО «iBank2» в порядке, установленном п.4.7. настоящего Регламента.
2.11. Клиент оплачивает предоставляемые Банком в соответствии с Договором услуги согласно Тарифам, действующим на момент оказания услуги. Оплата услуг по Договору производится путем списания денежных средств с Банковского счета Клиента в соответствии с Договором банковского счета.
2.12. Договор прекращает свое действие при закрытии Клиентом всех Банковских счетов, и/или расторжении Договоров банковского счета, в соответствии с которыми осуществляется обслуживание Клиента.
2.13. При невозможности обмена ЭД между Банком и Клиентом по Системе ДБО «iBank2» (сбои в работе оборудования, средств связи, приостановление работы Клиента в Системе ДБО «iBank2», отключение Клиента от Системы ДБО «iBank2» и т.п.) расчетно-кассовое обслуживание Клиента осуществляется путем обмена документами на бумажных носителях в соответствии с Договором банковского счета.

3. СОГЛАШЕНИЯ СТОРОН

3.1. Стороны признают, что используемые ими в соответствии с настоящим Регламентом СКЗИ и системы обработки, хранения, защиты и передачи информации достаточны для обеспечения надежной, эффективной и безопасной работы и защиты от несанкционированного доступа третьих лиц, а также для подтверждения авторства и подлинности ЭД, выявления фальсифицированных ЭД, при условии соблюдения Клиентом мер информационной безопасности в соответствии с Требованиями по обеспечению информационной безопасности при работе с Системой ДБО «iBank2», изложенными в Приложении 4 к настоящему Регламенту.
3.2. Клиент признает, что получение Банком ЭД, сформированного Клиентом в Системе ДБО «iBank2», заверенного ЭП Клиента, юридически эквивалентно получению Банком соответствующего документа на бумажном носителе, заверенного подписями и печатью Клиента, соответствующими образцам из карточки с образцами подписей и оттиском печати Клиента. Такой ЭД имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в соответствии с законодательством Российской Федерации и настоящим Регламентом.
3.3. ЭД признаются равнозначными документам на бумажном носителе, подписанным собственноручной подписью, при одновременном выполнении следующих условий:

- ЭД подписаны необходимым количеством ЭП ;
- проверка подлинности всех ЭП в ЭД дала положительный результат;
- СКП ЭП действуют на момент проверки.

3.5. Стороны признают надлежащим уведомление Клиента о совершенных Операциях с использованием способов, описанных в разделе 9 настоящего Регламента.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ ДБО «IBANK2»

4.1. Клиент обеспечивает организацию рабочего места, отвечающего Требованиям к комплексу программно-технических средств, необходимых для работы Системы ДБО «iBank2» (Приложение 3 к настоящему Регламенту), и Требованиям по обеспечению информационной безопасности при работе в Системе ДБО «iBank2» (Приложение 4 к настоящему Регламенту).
4.2. Подключение Клиента к Системе ДБО «iBank2» осуществляется на основании Заявления Клиента.
4.3. В соответствии с Тарифами Клиент оплачивает стоимость услуг по подключению к Системе ДБО «iBank2».

4.4. Банк предоставляет Клиенту требуемое количество Ключевых носителей по Акту приема-передачи (является приложением к Договору) и регистрирует в Журнале учета выдачи криптографической защиты информации количество Ключевых носителей (Приложение 2 к настоящему Регламенту).
4.5. Клиент проходит процедуру предварительной регистрации в Системе ДБО «iBank2». Указанная процедура осуществляется Клиентом самостоятельно в разделе «Регистрация» - «Подключение к системе» на странице входа в Систему ДБО «iBank2» в соответствии с Руководством по подключению к Системе ДБО «iBank2», размещенной на сайте Банка.
4.6. Во время предварительной регистрации Клиент формирует (генерирует) Ключи ЭП для представителей Клиента. При этом Ключи проверки ЭП автоматически сохраняются на сервере Системы ДБО «iBank2» в Банке.
В процессе генерации на каждый Ключ ЭП формируется СКП ЭП (Приложение 1 к настоящему Регламенту). СКП ЭП содержит следующую информацию:

- идентификатор Ключа проверки ЭП (уникальный номер СКП ЭП) (формируется автоматически);
- представление Ключа проверки ЭП в шестнадцатеричном виде (уникальный Ключ проверки ЭП) (формируется автоматически);
- даты начала и окончания срока действия СКП ЭП (заполняется сотрудником Банка при регистрации СКП ЭП);
- информацию, позволяющую идентифицировать Владельца СКП ЭП (для юридических лиц - наименование, ИНН, для физических лиц - ФИО, данные документа, удостоверяющего личность, иную информацию) (вводится Клиентом в процессе регистрации и генерации Ключа ЭП);
- наименование используемого средства ЭП (формируется автоматически);
- иную информацию, предусмотренную законодательством Российской Федерации. На каждый Ключ ЭП Клиент распечатывает СКП ЭП в двух экземплярах, проверяет правильность заполнения полей, заверяет личной подписью Владельца СКП ЭП в соответствующем поле. Достоверность приведенных в СКП ЭП данных подтверждается подписью лица, уполномоченного заверять СКП ЭП от имени Клиента, и печатью при ее наличии. Оба экземпляра СКП ЭП передаются в Банк для проверки и регистрации.

4.7. Уполномоченные сотрудники Банка в срок не более 2 (двух) рабочих дней после приема СКП ЭП проверяют правильность заполнения полей СКП ЭП Клиентом, вносят недостающие данные со стороны Банка, проставляют дату регистрации СКП ЭП в Системе ДБО «iBank2», подписи и заверяют штампами и печатями Банка, определенными для этих целей. Один экземпляр СКП ЭП остается в Банке, второй передается Клиенту. На основании СКП ЭП Банком производится окончательная регистрация Клиента в Системе ДБО «iBank2» путем регистрации СКП ЭП и активации Ключей проверки Владельцев СКП ЭП. Дата регистрации СКП ЭП, указанная в нем Банком, является датой начала работы Клиента в Системе ДБО «iBank2».
4.8. В случае неправильного заполнения СКП ЭП или неуспешной проверки документов на возвращаемом Клиенту экземпляре СКП ЭП на обратной стороне указывается причина отказа в регистрации. Клиент должен повторно выполнить генерацию Ключа ЭП и предоставить необходимые документы.

5. СРОК ДЕЙСТВИЯ КЛЮЧА ЭП. СМЕНА КЛЮЧЕЙ ЭП

5.1. При генерации Ключа ЭП в Системе ДБО «iBank2» Банком устанавливается срок действия Ключа ЭП, который соответствует сроку действия СКП ЭП, указанному в СКП ЭП. Максимальный срок действия СКП ЭП не может превышать 2 (Два) года со дня регистрации СКП ЭП в Системе ДБО «iBank2».

5.2. Действие СКП ЭП приостанавливается в случае истечения срока полномочий Владельца СКП ЭП. Срок полномочий Владельца СКП ЭП определяется на основании учредительных, организационно-распорядительных (приказов, трудовых договоров, протоколов заседаний органов управления, доверенностей) и иных документов, находящихся в Юридическом деле Клиента.
5.3. В Системе ДБО «iBank2» Банком осуществляется контроль срока действия СКП ЭП и срока полномочий Владельца СКП ЭП.
5.4. Банк посредством Системы ДБО «iBank2» уведомляет Владельца СКП ЭП о предстоящем истечении срока действия СКП ЭП за 30 (тридцать) календарных дней до даты окончания срока. При входе в Систему ДБО «iBank2» Владелец СКП ЭП получает уведомление с информацией о количестве дней, оставшихся до окончания срока действия СКП ЭП, и предложением сгенерировать новый Ключ ЭП.
5.5. Разблокировка Ключа ЭП, работа с которым приостановлена в соответствии с п. 5.2. настоящего Регламента, осуществляется не позднее рабочего дня, следующего за днем предоставления Клиентом в Банк документов, подтверждающих продление полномочий Владельца СКП ЭП.
5.6. Работа Клиента с Ключами ЭП осуществляется в разделе «Электронные подписи» Системы ДБО «iBank2». Владелец действующего СКП ЭП может просмотреть информацию о своих Ключах ЭП, переименовать или удалить Ключ ЭП, изменить пароль Ключа ЭП, проверить информацию, указанную в СКП ЭП.
5.7. Владельцы действующих СКП ЭП имеют возможность плановой генерации новых Ключей ЭП взамен Ключей ЭП, срок действия которых истекает, для регистрации СКП ЭП в виде электронного документа. Условиями выпуска СКП ЭП являются:

- действующий СКП ЭП;
- соответствие информации о Клиенте и Владельце СКП ЭП, указанной в новом СКП ЭП, информации, имеющейся в Юридическом деле Клиента.

Генерацию нового Ключа ЭП взамен Ключа ЭП, срок действия которого истекает (смену Ключа ЭП), рекомендуется осуществлять в срок не позднее, чем за 10 (десять) календарных дней до даты окончания срока его действия.
Уполномоченные сотрудники Банка в срок не более 2 (двух) рабочих дней после дистанционного выпуска СКП ЭП (получения от Клиента Заявления на выпуск сертификата ключа проверки, сформированного в Системе ДБО «iBank2») проверяют полномочия лица и актуальность паспортных данных. При положительном результате проверки новый СКП ЭП регистрируется в Системе ДБО «iBank2» и новые Ключи ЭП активируются. Срок действия СКП ЭП при плановой генерации новых Ключей ЭП начинается со дня активации новых Ключей ЭП.
С момента регистрации Банком нового СКП ЭП, СКП ЭП, срок действия которого истекает, аннулируется.
5.8. Кроме случая истечения срока действия СКП ЭП, действие СКП ЭП прекращается в случаях аннулирования СКП ЭП, указанных в 5.9. настоящего Регламента. Владельцам СКП ЭП, действие которого прекращено, работа с Ключом ЭП блокируется.
5.9. Банк аннулирует СКП ЭП самостоятельно или по заявлению Клиента по следующим основаниям:

- произведена регистрация Банком нового СКП ЭП взамен СКП ЭП, срок действия которого истекает;
- прекращены полномочия Владельца СКП ЭП как представителя Клиента;
- поврежден Ключевой носитель;
- не подтверждено, что Владелец СКП ЭП владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком СКП ЭП;
- при компрометации Ключа ЭП;
- в иных случаях невозможности пользования имеющимися Ключами ЭП.

5.10. К событиям, связанным с компрометацией Ключа ЭП, относятся следующие:

- утрата Ключевого носителя, в том числе с его последующим обнаружением;

- получение информации или возникновение подозрений о том, что Ключ ЭП стал доступен третьим лицам, а также об утечке информации или ее искажении в Системе ДБО «iBank2»;
- случаи, когда нельзя достоверно установить, что произошло с Ключевыми носителями (в том числе случаи, когда Ключевой носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- факт или попытка несанкционированного списания денежных средств со счета Клиента с использованием зарегистрированного(ных) Ключа(ей) ЭП;
- в случае получения Банком информации, содержащейся в БДБР о СБСК, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемы в соответствии с частью 8 статьи 27 Федерального закона № 161-ФЗ, на период нахождения указанных сведений в БДБР о СБСК;
- компрометация Средств доступа, в том числе получение информации или возникновение подозрений на получение третьими лицами доступа к логинам и паролям, на компрометацию среды исполнения (наличие в компьютере вредоносных программ, нестандартная работы системного программного обеспечения и т.д.);
- иные обстоятельства, прямо или косвенно свидетельствующие о доступе или возможности доступа к использованию Ключа ЭП неуполномоченными лицами.

5.11. Владельцы СКП ЭП, срок действия которых закончился (просрочен) или прекратился в случаях, указанных в 5.8. настоящего Регламента, а также Клиенты при генерации Ключа ЭП новому представителю проводят мероприятия по генерации нового Ключа ЭП в соответствии с 4.6. настоящего Регламента. В этом случае работа с Ключами ЭП осуществляется в разделе «Регистрация»-«Получение электронной подписи» Системы ДБО «iBank2».

6. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭП И/ИЛИ ВЫЯВЛЕНИИ ОПЕРАЦИЙ, СОДЕРЖАЩИХ ПРИЗНАКИ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА В РАМКАХ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ.

6.1. Банк в соответствии с Федеральным законом № 161-ФЗ осуществляет проверку наличия признаков осуществления перевода денежных средств с использованием Системы ДБО «iBank2» без добровольного согласия Клиента. При проверке наличия признаков осуществления перевода денежных средств с использованием Системы ДБО «iBank2» без добровольного согласия Клиента применяется порядок действий, установленный в главе 5, в приложении 4 к Правилам осуществления перевода денежных средств в Коммерческом Банке «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью), в настоящей главе, в главе 10 настоящего Регламента, а также во внутренних нормативных документах, регулирующих процессы автоматизированного мониторинга переводов денежных средств без добровольного согласия Клиента в рамках системы управления рисками.

6.2. Выявление Клиентом компрометации Ключей ЭП или подозрении на их компрометацию и/или выявление Клиентом использования Системы ДБО «iBank2» без его добровольного согласия и/или выявление Клиентом операций/ получения уведомления от Банка об операции, соответствующей признакам перевода денежных средств без добровольного согласия Клиента.

6.2.1. Клиент обязан незамедлительно направить уведомление в Банк в случаях, указанных в п.6.2 настоящего Регламента, способом, предусмотренн в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2».

6.2.2. При получении Банком уведомления, указанного в 6.2.1. настоящего Регламента, либо при получении Банком из любых иных источников информации о компрометации Ключа ЭП и/или использовании Системы ДБО «iBank2» без добровольного согласия Клиента, Банк незамедлительно приостанавливает доступ к Системе ДБО «iBank2» и исполнение любых ЭД.
Банк в день такого приостановления уведомляет Клиента о приостановлении доступа к Системе ДБО «iBank2» с указанием причины такого приостановления. Уведомление Клиенту предоставляется способом, предусмотренн в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2».
6.3. Выявление Банком операций, совершаемых в Системе ДБО «iBank2», с использованием автоматизированной Системы «Fraud-мониторинг» (предотвращения переводов денежных средств без добровольного согласия Клиента), соответствующих признакам переводов денежных средств без добровольного согласия Клиента:
6.3.1. Банк получает от Банка России информацию, содержащуюся в БДБР о СБСК, которая содержит сведения, относящиеся к Клиен и (или) его электронному средству платежа. Банк в рамках реализуемой системы управления рисками и в порядке, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», вправе приостановить использование клиентом электронного средства платежа на период нахождения сведений, относящихся к такому Клиенту и (или) его электронному средству платежа, в БДБР о СБСК.
6.3.2. Банк приостанавливает использование Клиентом электронного средства платежа, если от Банка России получена информация, содержащаяся в БДБР о СБСК, которая содержит сведения, относящиеся к Клиенту и (или) его электронному средству платежа, в том числе сведения федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, получаемые в соответствии с частью 8 статьи 27 Федерального закона № 161-ФЗ, на период нахождения указанных сведений в БДБР о СБСК.
6.3.3. После приостановления использования Клиентом электронного средства платежа в случаях, предусмотренных пп. 6.3.1. и 6.3.2. настоящего Регламента, Банк в порядке, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», незамедлительно уведомляет Клиента о приостановлении использования электронного средства платежа, а также о праве клиента подать в порядке, установленном Банком России, заявление в Банк России, в том числе через Банк, об исключении сведений, относящихся к Клиенту и (или) его электронному средству платежа, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из БДБР о СБСК.
6.3.4. В случае наличия у Банка оснований полагать, что включение сведений, относящихся к Клиенту и (или) его электронному средству платежа, в БДБР о СБСК является необоснованным, Банк вправе самостоятельно (без участия клиента) направить в Банк России мотивированное заявление об исключении сведений, относящихся к Клиенту и (или) его электронному средству платежа, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, из БДБР о СБСК.
6.3.5. Мотивированное решение об удовлетворении или об отказе в удовлетворении заявлений, указанных в пп 6.3.4. и 6.3.5. настоящей статьи, принимается в порядке, установленном Банком России, в срок, не превышающий 15 рабочих дней. Решение об отказе в удовлетворении таких заявлений может быть обжаловано в суд в соответствии с законодательством Российской Федерации.

6.3.6. В случае получения в порядке, установленном Банком России, информации об исключении сведений, относящихся к клиенту и (или) его электронному средству платежа, из БДБР о СБСК, Банк незамедлительно возобновляет использование клиентом электронного средства платежа и незамедлительно уведомляет Клиента о возможности использования электронного средства платежа при отсутствии иных оснований для приостановления использования электронного средства платежа Клиента в соответствии с законодательством Российской Федерации или договором.
6.4. С момента приостановления использования Клиентом Системы ДБО «iBank2» прием документов Клиента осуществляется только на бумажном носителе.
6.5. Права и обязанности Сторон в части порядка действий при компрометации ключей ЭП и/или выявлении операций, содержащих признаки перевода денежных средств без добровольного согласия Клиента, установлены в главе 10 данного Регламента.

7. ПОРЯДОК ОБМЕНА (ДОКУМЕНТООБОРОТА) ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ И ИНФОРМАЦИЕЙ В СИСТЕМЕ ДБО «IBANK2»

7.1.Система ДБО «iBank2» позволяет:

- осуществлять прием от Клиента созданных, подписанных ЭП и отправленных в Банк Платежных ЭД Клиента;
- осуществлять прием от Клиента подписанных ЭП ЭД свободного формата (заявлений, справок, уведомлений, реестров и проч.);
- получать и просматривать информацию (выписки Банка) об Операциях, иные уведомления и извещения, в том числе, направление которых для Банка является обязательным в соответствии с законодательством Российской Федерации;
- осуществлять просмотр информации о ЭД, поступивших в Банк в целях осуществления перевода денежных средств со счетов Клиента, о статусах ЭД, просмотр уведомлений об их исполнении (неисполнении);

7.2. В рамках Системы ДБО «iBank2» Клиент и Банк может обмениваться следующими видами ЭД:

- Платежные документы;
- Заявка на наличные;
- Входящие платежные требования и инкассовые поручения;
- Заявление на перевод валюты;
- Поручение на покупку иностранной валюты;
- Поручение на продажу иностранной валюты;
- Распоряжение на обязательную продажу иностранной валюты;
- Распоряжение на списание с транзитного счета;
- Запрос на отзыв ЭД;
- Документы, перечисленные в Инструкции Банка России от 16.08.2017 № 181-И «О порядке представления резидентами и нерезидентами уполномоченным банкам подтверждающих документов и информации при осуществлении валютных операций, о единых формах учета и отчетности по валютным операциям, порядке и сроках их представления»;
- Уведомление о зачислении иностранной валюты на транзитный валютный счет Клиента;
- Документы, установленные внутренними регламентами Банка, в целях осуществления контроля за операциями с денежными средствами и иным имуществом, предусмотренными Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ);
- Документы свободного формата (запросы, тексты, сообщения свободного формата);

- Прочие документы и приложения к ним, определенные заключенными сторонами договорами или соглашениями.

7.3. Перечень документов, передаваемых по Системе ДБО «iBank2», Банк вправе изменять в одностороннем порядке.

7.4.Этапы электронного документооборота:

- формирование ЭД, заверение его ЭП;
- отправка и доставка ЭД;
- проверка ЭД;
- подтверждение получения ЭД Банком;
- учет ЭД (регистрация входящих и исходящих ЭД в Системе ДБО «iBank2»);
- хранение ЭД (ведение архивов ЭД).

7.5. Система ДБО «iBank2» автоматически отображает сведения о текущем этапе (стадии) обработки Клиентом и/или Банком ЭД посредством присвоения ЭД определенного статуса. Статус каждого ЭД, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами Системы ДБО «iBank2» во время сеансов связи, проводимых Клиентом. Свидетельством того, что ЭД принят Банком для проведения процедуры приема к исполнению в соответствии с законодательством Российской Федерации и утвержденным в Банке порядком, является присвоение ему в Системе статуса «доставлен».

7.6. В Системе ДБО «iBank2» возможно присвоение следующих статусов ЭД:

- **«новый»:** присваивается при создании и сохранении нового ЭД, при редактировании и сохранении существующего ЭД, а также при импорте ЭД из файла. ЭД со статусом «новый» Банк не рассматривает и не обрабатывает;
- **«доставлен»:** присваивается ЭД, когда число подписей под документом соответствует необходимому для рассмотрения документа Банком. Статус «доставлен» является для Банка указанием начать обработку ЭД (исполнить или отвергнуть);
- **«на обработке»:** присваивается ЭД при его выгрузке в АБС после прохождения всех ее проверок;
- **«на исполнении»:** присваивается при принятии ЭД к исполнению (проведении Банком процедуры приема к исполнению в соответствии с действующим законодательством Российской Федерации и порядком, утвержденным в Банке);
- **«исполнен»:** присваивается ЭД непосредственно после отражения документа в балансе Банка;
- **«отвергнут»:** присваивается ЭД, не прошедшему проверку АБС, либо последующую проверку по причине его несоответствия требованиям, установленным действующим законодательством Российской Федерации или настоящим Регламентом, а также в иных случаях на усмотрение Банка. Клиент может создать новый ЭД на основе отвергнутого или удалить ЭД.
- **«удален»:** присваивается ЭД, удаленному Клиентом. ЭД, удаленные из системы после отвержения, можно просмотреть, используя фильтр в информационной панели интерфейса.

7.7. Формирование ЭД осуществляется в следующем порядке:

7.7.1. ЭД формируется путем заполнения стандартной формы, предусмотренной в Системе ДБО «iBank2» или при загрузке файлов соответствующего формата, сформированных внешними программами. При формировании ЭД Система ДБО «iBank2» осуществляет автоматический контроль присутствия обязательной информации в соответствующих полях формы документа. Ключевыми полями ЭД являются все обязательные для данного вида ЭД реквизиты, без наличия которых надлежащее исполнение ЭД является невозможным.

7.7.2. Возможно формирование ЭД, не являющегося платежным, в виде текстового (в формате DOC, RTF, TXT и др.) или графического (в форматах PDF, JPEG/JPG, TIF и др.) документа для дальнейшей пересылки в Банк в виде вложения в ЭД «Письмо» или в другие виды ЭД, в которых предусмотрена возможность присоединения файлов.
7.7.3. Сформированный ЭД подписывается ЭП. ЭП подтверждает авторство ЭД, созданного в Системе ДБО «iBank2», и является средством проверки неизменности его содержания. При подписи ЭД с вложенными файлами одновременно подписываются присоединенные к ЭД файлы. ЭД с присоединенными файлами представляет собой единое целое.
7.7.4. В соответствии с Заявлением Клиента могут устанавливаться ограничени на осуществление операций в Системе ДБО «iBank2» (список получателей, в пользу которых регулярно совершаются платежи, лимит по сумме платежей для каждого такого получателя и другие).
7.8.Проверка ЭД включает:

- проверку ЭД на соответствие установленному формату для данного вида ЭД;
- проверку подлинности и актуальности всех ЭП электронного документа;
- проверку соответствия параметров ЭД требованиям Договоров, заключенных между Банком и Клиентом, а также действующему законодательству Российской Федерации и нормативным актам Банка России.

7.9. В отношении платежных ЭД Клиента Банк дополнительно проводит процедуры приема к исполнению, установленные законодательством Российской Федерации, правилами осуществления перевода денежных средств и Договором банковского счета.
7.10. ЭД считается исходящим от Клиента, если:

- подписан с использованием Ключей ЭП Клиента;
- срок действия СКП ЭП не истек;
- Банк не уведомлен о компрометации Ключей ЭП Клиента;
- срок полномочий Владельцев СКП ЭП, указанный в документах, представленных Клиентом и находящихся в Юридическом деле Клиента, не истек;
- ЭД передан в Банк посредством Системы ДБО «iBank2».

В случае положительного результата проверки ЭД присваивается статус «доставлен» или «на обработке», и он принимается к исполнению.
В случае отрицательного результата проверки, ЭД не может быть принят к исполнению и ЭД присваивается статус «отвергнут».
7.11. Клиент может отозвать отправленный ЭД со статусом «доставлен», «на обработке» или «на исполнении», направив в Системе ДБО «iBank2» запрос на отзыв с указанием причины отзыва.
7.12. Клиент обязан по рабочим дням, до момента получения информации об исполнении либо об отказе в исполнении ЭД, отслеживать информацию об этапах и результатах обработки ЭД в соответствующих разделах Системы ДБО «iBank2».
7.13. При отсутствии изменения статуса ЭД в Операционное время в течение 2 (двух) часов с момента отправки ЭД в Банк Клиент обязан уведомить Банк о данном факте в день отправки ЭД любым доступным способом, позволяющим идентифицировать Клиента. Банк не несет ответственность за неисполнение неполученных или непринятых ЭД.
7.14. Ответственность за риски, возникающие в случае отсутствия или несвоевременного контроля Клиентом за результатами обработки ЭД, несет Клиент.
7.15. Свидетельством того, что ЭД исполнен Банком, является присвоение ему в Системе ДБО «iBank2» статуса «исполнен». После присвоения статуса «исполнен» ЭД отражается в электронной выписке по Банковскому счету.
7.16. В случае непринятия (отказа в принятии) ЭД Клиента ему присваивается статус «отвергнут» с указанием причины отвержения. Клиенту направляется сообщение об отказе в исполнении ЭД (позволяющее идентифицировать ЭД, дату и основание отказа).

7.17. Прием ЭД, передаваемых Клиентом посредством Системы ДБО «iBank2», производится Банком в автоматическом режиме.

8. ДЕЙСТВИЯ БАНКА В СЛУЧАЕ ПОЛУЧЕНИЯ УВЕДОМЛЕНИЯ О ПРИОСТАНОВЛЕНИИ ЗАЧИСЛЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ

8.1. В случае получения Банком от оператора по переводу денежных средств, обслуживающего плательщика, уведомления о приостановлении зачисления денежных средств на Банковский счет Клиента до осуществления зачисления денежных средств на Банковский счет Клиента, Банк обязан приостановить на срок до 5 (пяти) рабочих дней со дня получения такого уведомления зачисление денежных средств на Банковский счет Клиента в сумме перевода денежных средств и незамедлительно уведомить Клиента о приостановлении зачисления денежных средств на его Банковский счет и необходимости представления в пределах 5 (пяти) рабочих дней документов, подтверждающих обоснованность получения переведенных денежных средств. Уведомление Клиента о приостановлении зачисления денежных средств Банк осуществляет в порядке, указанном в п. 6.2 настоящего Регламента.
8.2. В случае представления в течение 5 (пяти) рабочих дней со дня совершения Банком,
действий, предусмотренных п.8.1. настоящего Регламента, Клиентом документов, подтверждающих обоснованность получения переведенных денежных средств, Банк обязан осуществить зачисление денежных средств на Банковский счет Клиента.
8.3. В случае непредставления в течение 5 (пяти) рабочих дней со дня совершения Банком действий, предусмотренных п.8.1. настоящего Регламента, Клиентом документов, подтверждающих обоснованность получения переведенных денежных средств или их проверки с отрицательным результатом, Банк обязан осуществить возврат денежных средств оператору по переводу денежных средств, обслуживающему плательщика, не позднее 2 (двух) рабочих дней после истечения указанного пятидневного срока.
8.4. В случае получения от оператора по переводу денежных средств, обслуживающего плательщика, уведомления о приостановлении после осуществления зачисления денежных средств на Банковский счет Клиента Банк направляет оператору по переводу денежных средств, обслуживающему плательщика, уведомления о невозможности приостановления зачисления денежных средств на Банковский счет Клиента.

9. ПОРЯДОК ИНФОРМИРОВАНИЯ КЛИЕНТОВ О СОВЕРШЕНИИ ОПЕРАЦИЙ В СИСТЕМЕ ДБО «IBANK2»

9.1. Информирование Клиента о совершении Операций в Системе ДБО «iBank2» осуществляется путем предоставления через WEB-интерфейс Системы ДБО «iBank2» в режиме онлайн информации об Операциях Клиента путем присвоения Банком статусов ЭД, а также выписок по Банковским счетам Клиента.
9.1.1. Актуальными сведениями о телефонном номере и электронном адресе Клиента является информация, указанная в карточке Клиента в АБС Банка.
9.1.2. Для получения оперативной информации по совершенным Операциям и остаткам на Банковских счетах, а также для получения информации по Операциям на Банковском счете за конкретный период Клиент имеет возможность получать выписки в соответствующем разделе Системы ДБО «iBank2», указывая номера Банковских счетов и интересующий период. Электронная выписка, полученная в течение текущего операционного дня, является предварительной и может быть изменена Банком. Окончательная выписка по Банковскому счету предоставляется не позднее 12:00 следующего операционного дня.

9.1.3. Клиент обязан самостоятельно на регулярной основе (не реже 1 (одного) раза в сутки) производить контроль за произошедшими операциями и присвоенными им статусами ЭД посредством Системы ДБО «iBank2».
9.1.4. Клиент вправе в любой момент внести изменения в сведения об актуальном номере телефона и электронном адресе.
9.2. Клиент признает надлежащим способ информирования о совершении Операций, путем присвоения статусов ЭД Системе ДБО «iBank2».
9.3. Обязанность Банка по информированию Клиента считается исполненной в момент предоставления через WEB-интерфейс Системы ДБО «iBank2» в режиме онлайн информации об Операциях Клиента путем присвоения Банком статусов ЭД, а также выписок по Банковским счетам Клиента.

10. ПРАВА И ОБЯЗАННОСТИ СТОРОН

10.1.Взаимные права и обязанности Сторон:

10.1.1. Стороны обязуются при проведении электронных расчетов с использованием Системы ДБО «iBank2» руководствоваться правилами и требованиями, установленными законодательством Российской Федерации и настоящим Регламентом.
10.1.2. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для обмена ЭД по Системе ДБО «iBank2» в соответствии с настоящим Регламентом.
10.1.3. Стороны обязуются не разглашать третьим лицам (за исключением случаев, предусмотренных законодательством Российской Федерации или дополнительным соглашением Сторон) конкретные способы защиты информации, реализованные в Системе ДБО «iBank2».
10.1.4. Стороны обязуются организовать режим работы сервисов Системы ДБО «iBank2» таким образом, чтобы исключить возможность использования сервисов лицами, не имеющими соответствующего разрешения для работы с ними, а также исключить возможность использования технических, программных и коммуникационных ресурсов неуполномоченными лицами.
10.1.5. Стороны обязуются сохранять в тайне применяемые в Системе ДБО «iBank2» Ключи ЭП и своевременно проводить их замену в порядке, предусмотренном настоящим Регламентом.
10.1.6. Каждая Сторона имеет право запрашивать и обязана предоставлять по запросам другой Стороны надлежащим образом оформленные бумажные копии ЭД.

10.2. Клиент имеет право:

10.2.1. Отправлять в Банк ЭД, предусмотренные Системой ДБО «iBank2», и пользоваться предоставляемыми Системой ДБО «iBank2» сервисами. Оформление документов должно соответствовать требованиям, установленным действующим законодательством, соответствующими договорами и настоящим Регламентом.
10.2.2. В случае неработоспособности Системы ДБО «iBank2» оформлять и передавать в Банк документы на бумажных носителях.
10.2.3. По своему усмотрению генерировать новые Ключи ЭП Владельцев СКП ЭП Клиента и регистрировать в Банке новые СКП ЭП.
10.2.4. Устанавливать в соответствии с Заявлением ограничения на осуществление операций в Системе ДБО «iBank2».
10.2.5. В случае несогласия с Операцией или в случае возникновения претензий, связанных с принятием к обработке / исполнением ЭД, предоставлять в Банк мотивированное заявление о разногласиях, руководствуясь 12.4 настоящего Регламента.

10.2.6. Направить в Банк, в случае выявления операции/получения уведомления об операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с требованиями Федерального Закона № 161-ФЗ информацию способом, предусмотренн в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2».

10.3. Клиент обязан:

10.3.1. Самостоятельно знакомиться с условиями действующего Регламента и Тарифов, строго соблюдать требования Системы ДБО «iBank2», изложенные в настоящем Регламенте.
10.3.2. Предоставить Банку достоверную информацию для связи с Клиентом (уполномоченными лицами), а в случае ее изменения незамедлительно предоставить обновленную информацию. Обязанность Банка по направлению Клиенту уведомлений, предусмотренных законодательством Российской Федерации и настоящим Регламентом, считается исполненной при направлении уведомлений в соответствии с имеющейся у Банка информацией для связи с Клиентом.
10.3.3. Своевременно уведомить Банк о компрометации Ключей ЭП, выявлении использования Системы ДБО «iBank2» без добровольного согласия Клиента, выявлении операций, содержащих признаки перевода денежных средств без добровольного согласия Клиента. В случае компрометации Ключей ЭП инициировать процедуру смены Ключей ЭП, конфиденциальность которых потенциально нарушена, в порядке, установленном разделом 6 настоящего Регламента.
10.3.4. Оплачивать оказанные Банком с использованием сервисов Системы ДБО «iBank2» услуги в соответствии с Тарифами, действующими на день оказания услуги. При наступлении срока взимания комиссий (вознаграждения), предусмотренных Тарифами, обеспечить на Банковском счете остаток денежных средств, достаточный для уплаты сумм комиссий, причитающихся Банку.
10.3.5. Иметь в наличии комплекс программно-технических средств, необходимых для работы Системы ДБО «iBank2», отвечающий требованиям, изложенным в Приложении 3 к настоящему Регламенту. Клиент настоящим подтверждает, что извещен о том, что изменение конфигурации программно-технических средств на его стороне может привести к сбою в работе Системы ДБО «iBank2».
10.3.6. Следовать требованиям Банка по обеспечению безопасности при работе с сервисами Системы ДБО «iBank2», изложенным в инструкциях по эксплуатации и в Приложении 4 к настоящему Регламенту, в том числе обеспечить хранение Ключевых носителей в местах, исключающих доступ неуполномоченных лиц и возможность их повреждения.
10.3.7. В связи с тем, что эксплуатируемые программы и технологии, а также данные, образующиеся в результате работы программного обеспечения, содержат конфиденциальную информацию, Клиент обязуется всеми доступными ему способами, предотвращать доступ к информации, связанной с работой Системы ДБО «iBank2» не допущенных к ней лиц.
10.3.8. Контролировать правильность реквизитов, указываемых в ЭД, и отслеживать изменение статуса ЭД, отправленных в Банк посредством Системы ДБО «iBank2».
10.3.9. Извещать Банк об изменениях данных, указанных в Заявлении и в своих учредительных документах, изменении/прекращении полномочий одного или нескольких Владельцев СКП ЭП в срок, установленный в заключенных с Банком договорах. В противном случае Банк руководствуется имеющимися в его распоряжении документами и не несет ответственность за возможные негативные последствия.
10.3.10. В день подключения к Системе ДБО «iBank2» проверить верность реквизитов Клиента в Системе ДБО «iBank2», а также верность сведений, указанных в атрибутах СКП ЭП, и незамедлительно сообщить в Банк в случае несоответствия вышеуказанных реквизитов.

10.4. Банк имеет право:

10.4.1. Изменять настоящий Регламент и Тарифы в одностороннем порядке.

10.4.2. Списывать с банковского(их) счета(ов) Клиента сумму платежей за услуги, оказанные с использованием сервисов Системы ДБО «iBank2», в соответствии с Тарифами, действующими на день оказания услуги.

10.4.3. В одностороннем порядке вводить дополнительные меры информационной безопасности, аутентификации, авторизации и идентификации Клиента в Системе ДБО «iBank2».

10.4.4. По своему усмотрению настраивать и расширять перечень предоставляемых услуг с использованием Системы ДБО «iBank2».

10.4.5. Осуществлять обновление программного обеспечения, устанавливать технические и иные ограничения работы сервисов Системы ДБО «iBank2» в целях соблюдения требований законодательства Российской Федерации, обеспечения безопасности совершения Операций без дополнительного уведомления Клиента. При этом в обязательном порядке производятся обновления, направленные на устранение ставших известными Банку уязвимостей программного обеспечения.

10.4.6. Отказать Клиенту в заключении Договора.

10.4.7. Отказать Клиенту в обслуживании с использованием Системы ДБО «iBank2» в случае несогласия Клиента с использованием предложенных Банком средств доступа и подтверждения Операций.

10.4.8. Отказать в исполнении ЭД Клиента, переданного посредством Системы ДБО «iBank2», в случаях, предусмотренных законодательством Российской Федерации, в том числе, но не ограничиваясь, Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» и Федеральным законом № 115-ФЗ.

10.4.9. Уведомить в письменной форме по Системе ДБО «iBank2» о приостановлении использования Клиентом Системы ДБО «iBank2» в случае возникновения подозрения о том, что Операции осуществляются с целью легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и финансирования распространения оружия массового уничтожения, а также в случае, если в установленные сроки не были представлены в полном объеме документы и информация, запрошенные Банком, необходимые для исполнения требований Федерального закона № 115-ФЗ, включая информацию о своих выгодоприобретателях и бенефициарных владельцах.

Указанное в настоящем подпункте приостановление использования Клиентом Системы ДБО «iBank2» не является отказом в выполнении распоряжения о совершении операции в соответствии с законодательством Российской Федерации в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

С момента приостановления использования Клиентом Системы ДБО «iBank2» прием документов Клиента осуществляется только на бумажном носителе.

10.4.10. Без предварительного уведомления Клиента приостановить использование Системы ДБО «iBank2» в следующих случаях:

- при возникновении у Банка технических неисправностей или других обстоятельств, препятствующих использованию Системы ДБО «iBank2», обеспечению требуемого уровня безопасности при проведении Операций посредством Системы ДБО «iBank2»;
- при получении Банком информации о компрометации Ключа ЭП и/или использовании Системы ДБО «iBank2» без добровольного согласия Клиента и/или совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента;
- в случае выявления и непредставления Клиентом актуальной информации для связи с ним;
- в иных случаях, предусмотренных настоящим Регламентом.

10.4.11. Проводить регламентные работы по техническому обслуживанию аппаратно-программных средств Системы ДБО «iBank2». Работы выполняются строго вне рамок Операционного времени. В случае если регламентные работы влияют на уровень доступности сервисов Системы ДБО «iBank2», Банк оповещает Клиентов о планируемых регламентных работах, причинах и сроках их проведения информационным сообщением с использованием Системы ДБО «iBank2» не позднее, чем за 1 (один) календарных дня до начала работ.
10.4.12. Запрашивать у Клиента в дополнение к подтверждению в соответствии с п.10.5.7 настоящего Регламента информацию, что перевод денежных средств не является переводом без добровольного согласия Клиента, и документы, подтверждающие обоснованность получения денежных средств.
10.4.13. Приостановить использование Клиентом Системы ДБО «iBank2» в случае, если Банк получил от Банка России информацию, содержащуюся БДБР о СБСК, которая содержит сведения, относящиеся к Клиенту, на период нахождения таких сведений БДБР о СБСК в рамках реализуемой им системы управления рисками и уведомить Клиента способами, определенными в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2».

10.5. Банк обязан:

10.5.1. Обеспечить надлежащее функционирование Системы ДБО «iBank2» и минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе Системы ДБО «iBank2».
10.5.2. Подключить Клиента к Системе ДБО «iBank2» в соответствии с разделом 4 настоящего Регламента.
10.5.3. При изменении настоящего Регламента и Тарифов известить Клиента способом, указанным в 2.4 настоящего Регламента.
10.5.4. Осуществлять консультирование по вопросам эксплуатации Системы ДБО «iBank2» в течение срока действия Договора способом, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2»
10.5.5. Приостановить прием к исполнению Распоряжения ЭД при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с требованиями Федерального закона № 161-ФЗ на 2 (два) календарных дня, следующих за днем поступления в Банк Распоряжения ЭД Клиента.
10.5.6. Уведомлять Клиента в порядке, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2» о приостановлении приема к исполнению Распоряжения ЭД и/или приостановления зачисления в случае выявления операции/получении уведомления об операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента в соответствии с требованиями Федерального закона № 161-ФЗ, а также предоставлять Клиенту информацию о рекомендациях по снижению рисков повторного осуществления перевода без добровольного согласия Клиента и возможности подтвердить Распоряжение ЭД, прием к исполнению которого был приостановлен, не позднее одного календарного дня, следующего за днем приостановления приема к исполнению указанного Распоряжения ЭД.
10.5.7. Запрашивать у Клиента подтверждение исполнения Распоряжения ЭД при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента.

Незамедлительно принять к исполнению Распоряжение ЭД Клиента, прием к исполнению которого был приостановлен при выявлении Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента при получении от Клиента подтверждения посредством направления в Банк подтверждения Распоряжения ЭД способом, предусмотренным в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», при условии отсутствия в БДБР о СБСК, информации, относящейся к получателю средств по Распоряжению ЭД, а также при отсутствии иных установленных законодательством РФ и настоящим Регламентом оснований не принимать Распоряжение ЭД Клиента к исполнению.

В случае поступления подтверждения от Клиента в выходной/праздничный день, то Распоряжение ЭД принимается к исполнению в первый рабочий день, следующий за таким выходным/праздничным днем.

10.5.8. Не принимать к исполнению Распоряжение ЭД Клиента при неполучении от Клиента подтверждения Распоряжения ЭД и/или информации, дополнительно запрошенной Банком в соответствии с п.10.4.12 настоящего Регламента, способом, предусмотренным в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», в случае если прием к исполнению Распоряжения ЭД был приостановлен при выявлении Банком признаков осуществления перевода денежных средств без добровольного согласия Клиента.

10.5.9. Приостановить прием к исполнению подтвержденного Распоряжения ЭД на 2 (два) календарных дня со дня направления Клиентом подтверждения Распоряжения ЭД в порядке, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», в случае получения от Банка России информации, содержащейся в БДБР о СБСК, относящейся к получателю средств по подтвержденному Распоряжению ЭД, и уведомить Клиента любым доступным способом,

предусмотренным в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2», с указанием причины и срока приостановления.

10.5.10. Принять к исполнению подтвержденное Распоряжение ЭД Клиента, прием к исполнению которого был приостановлен в соответствии с п. 10.5.9 настоящего Регламента, незамедлительно по истечении 2 (двух) календарных дней со дня направления Клиентом подтверждения Распоряжения ЭД в порядке, установленном в Договоре с Клиентом, при отсутствии иных установленных законодательством и настоящим Регламентом оснований не принимать Распоряжение ЭД Клиента к исполнению.

Если истечение указанного срока выпадает на выходной/праздничный день, то подтвержденное Распоряжение ЭД принимается к исполнению в первый рабочий день, следующий за таким выходным/праздничным днем.

10.5.11. Приостановить использование Клиентом использование системы ДБО «iBank2» на период нахождения в БДБР о СБСК, сведений, относящихся к Клиенту, в том числе сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях сведений, и уведомить Клиента способами, определенными в Договоре с клиентом, о приостановлении обслуживания по Системе ДБО «iBank2», а также о праве Клиента подать в порядке, установленном Банком России, заявление в Банк России об исключении сведений, относящихся к Клиенту из Базы данных Банка России.

Банк незамедлительно возобновляет обслуживание по Системе ДБО «iBank2» по факту исключения из Базы данных Банка России, сведений, относящихся к Клиенту и уведомляет Клиента способами, определенными в Договоре с Клиентом , о возобновлении обслуживания по Системе ДБО «iBank2»

10.5.12. По факту получения от Клиента информации о Компрометации в соответствии с или в случае выявления Банком факта Компрометации/любых подозрений на Компрометацию при наличии у Банка информации о событиях, относящихся к Компрометации, Банк незазмедлительно блокирует скомпрометированный Ключ ЭП Клиента Системе ДБО «iBank2», прекращает прием и исполнение Распоряжений ЭД, подписанных скомпрометированным ключом ЭП.
Фактом уведомления Клиента является факт исполнения Заявления о компрометации, либо направление уведомления способом, предусмотренным в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2»
10.5.13. Возместит в течение 30 (тридцати) календарных дней Клиенту сумму операции, совершенной без добровольного согласия Клиента на основании полученного от Клиента заявления (уведомления) о несогласии с операцией, содержащего указание на совершение операции с использованием Системы ДБО «iBank2», в порядке, предусмотренном в Договоре между Банком и Клиентом об использовании Системы ДБО «iBank2».
10.5.5. Рассматривать заявления (уведомления) Клиента, связанные с использованием Системы ДБО «iBank2», и сообщать о результатах рассмотрения в письменной форме в срок не более 30 (тридцати) календарных дней со дня получения таких заявлений, а в случае осуществления трансграничного перевода денежных средств - в срок не более 60 (шестидесяти) календарных дней со дня получения заявления.
10.5.6. Обеспечить конфиденциальность информации, передаваемой в соответствии с настоящим Регламентом и Договором банковского счета.
10.5.7. Вести архивы ЭД и информации, связанной с обслуживанием в Системе ДБО «iBank2», в соответствии с законодательством Российской Федерации и внутренними правилами Банка.
Фиксировать направленные Клиенту и полученные от Клиента уведомления, хранить соответствующую информацию не менее трех лет.
10.5.8. Обеспечить информационную безопасность Системы ДБО «iBank2» в соответствии с законодательством Российской Федерации.

11. ОТВЕТСТВЕННОСТЬ СТОРОН

11.1. Стороны несут ответственность за ненадлежащие исполнение своих обязанностей в соответствии с законодательством Российской Федерации и условиями Договора.
11.2. Банк и Клиент не несут ответственности за убытки, понесенные одной Стороной не по вине другой Стороны в результате использования Системы ДБО «iBank2», в том числе при исполнении ошибочных ЭД, если эти ЭД надлежащим образом Клиентом оформлены и переданы, а Банком получены, проверены и признаны верными.
11.3. Банк обязан возместить Клиенту сумму Операции:
- совершенной без добровольного согласия Клиента после получения Банком уведомления Клиента, указанного в 6.2.1 настоящего Регламента.
- совершенной без добровольного согласия Клиента, о которой Клиент не был проинформирован Банком в порядке, предусмотренном разделом 9 настоящего Регламента.

11.4. Банк не обязан возместить Клиенту сумму Операции, совершенной без добровольного согласия Клиента, в случае если Банк проинформировал Клиента о совершенной Операции в порядке, предусмотренном разделом 9 настоящего Регламента, и Клиент не направил Банку уведомление в порядке, установленном Договором с Клиентом.
11.5. Клиент несет полную ответственность за сохранение в тайне информации о Средствах доступа, Кодах подтверждения и обязуется исключить доступ к ним третьих лиц.
11.6. Клиент несет ответственность за правильность заполнения и корректное содержание ЭД, переданных в Банк посредством Системы ДБО «iBank2».

11.7. Банк не несет ответственность за неработоспособность оборудования и каналов связи Клиента, повлекших за собой невозможность доступа Клиента к Системе ДБО «iBank2».
11.8. Банк не несет ответственности в случае финансовых потерь, понесенных Клиентом, в результате нарушения и/или ненадлежащего исполнения Клиентом Договора, а также несоблюдения требований по защите АРМ Клиента от Вредоносного кода, в том числе, но не ограничиваясь, в случае умышленной или неосторожной компрометации Клиентом применяемых в Системе ДБО «iBank2» Ключей ЭП Клиента, конфиденциальной информации и/или используемого программного обеспечения.
11.9. Банк не несет ответственности за скорость и факт доставки Клиенту информации, переданной через каналы передачи данных, находящиеся вне ведения Банка.
11.10. Клиент полностью несет все риски, связанные с подключением его оборудования (в том числе компьютерного) к сети Интернет. Клиент самостоятельно обеспечивает защиту данного оборудования от несанкционированного доступа и вирусных атак из сети Интернет.
11.11. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникшей в результате событий чрезвычайного характера, которые имели непредвиденный и (или) непредотвратимый при данных условиях характер, наступили после даты подписания Договора, непосредственно повлияли на его исполнение и которые Стороны не могли предвидеть.
11.12. Сторона по Договору, ссылающаяся на обстоятельства непреодолимой силы, обязана в течение 3 (трех) рабочих дней информировать другую Сторону о наступлении подобных обстоятельств, а также об оценке их влияния на исполнение своих обязательств по Договору и на срок исполнения этих обязательств.

12. РАЗРЕШЕНИЕ СПОРОВ

12.1. Споры и разногласия, связанные с выполнением Договора, разрешаются Сторонами путем переговоров. Обязательным для Сторон является соблюдение досудебного претензионного порядка урегулирования спора: претензия (и ответ на нее) должны направляться Сторонами друг другу в письменной форме, заказным письмом с уведомлением о вручении.
12.2. Разногласия, по которым Сторонами не достигнуты договоренности, подлежат рассмотрению судом в соответствии с законодательством Российской Федерации.
12.3. Приостановление или прекращение использования Клиентом Системы ДБО «iBank2», не прекращает обязательств Клиентов и Банка, возникших до момента приостановления или прекращения указанного использования.
12.4. При несогласии со списанием денежных средств по Операции, проведенной с использованием Системы ДБО «iBank2», Клиент направляет в Банк заявление о совершении спорной Операции.
12.5. Порядок предъявления, приема, регистрации, рассмотрения обращений Клиентов и направления ответов Банком на обращения Клиентов, перечень необходимой информации, указываемой в обращении, информация для связи, сроки рассмотрения обращений Клиентов установлен Порядком рассмотрения обращений клиентов в Коммерческом Банке «Республиканский Кредитный Альянс» (общество с ограниченной ответственностью), который вместе с Памяткой для клиентов размещается в месте обслуживания Клиентов.
12.6. Порядок проведения технической экспертизы при возникновении спорных ситуаций, связанных с использованием Системы ДБО «iBank2», установлен в приложении № 1 к Договору на обслуживание Клиентов в Системе ДБО «iBank2».

13. ПРОЧИЕ УСЛОВИЯ

13.1. Настоящий Регламент вступает в силу с момента подписания его уполномоченным органом Банка и действует до его отмены. В настоящий Регламент могут быть внесены изменения и дополнения в установленном порядке.

13.2. В случае изменения нормативно-правовых актов настоящий Регламент действует в части, не противоречащей действующему законодательству Российской Федерации и действующим нормативным документам Банка России.

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

1. Наименование организации _____

_____

2. Место нахождения юр. лица _____

_____

3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* "____" _____ года

4. ИНН (КИО) _____ 5. КПП* _____

6. Тел. _____ 7. Факс* _____ 8. E-mail* _____

9. Сведения о владельце ключа

Фамилия, имя, отчество _____

Должность _____

Документ, удостоверяющий личность _____

_____

серия _____ номер _____ дата выдачи "____" июня _____ года

кем выдан _____

код подразделения _____

10. Примечания* _____

* необязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____

подпись

Ключ проверки ЭП сотрудника клиента

Идентификатор ключа проверки ЭП _____ Идентификатор устройства _____

Наименование криптосредств СКЗИ "MS_KEY K" - "АНГАРА" Исп.8.1.1

Алгоритм ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком):

с "____" _____ 20__г.

по "____" _____ 20__г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание в системе "iBank" N___ от "__"_____20__ г.

Достоверность приведенных данных подтверждаю

Руководитель организации

_____/_____/

подпись Ф.И.О.

Оттиск печати

Уполномоченный представитель банка

_____/_____/

подпись Ф.И.О.

Оттиск печати Банка

Дата приема сертификата ключа проверки ЭП

"___"_____20__г.

Администратор безопасности системы

_____/_____/

подпись Ф.И.О.

Оттиск печати

Дата регистрации сертификата ключа проверки ЭП

"___"_____20__г.

Приложение 2

Журнал учета криптографической защиты информации для «iBank2»

№ п/п	Номера экземпляров (криптографические номера) ключевых носителей	Наименование системы криптографической защиты	Дата выдачи	Кем выдано
1	**2**	**3**	**4**	**5**

Название организации / ИП	Ф.И.О. представителя получающего криптографическую защиту	Подпись представителя	Дата ввода эксплуатацию	Примечание
6	**7**	**8**	**9**	**10**

Приложение 3

Требования к комплексу программно-технических средств необходимых для работы Системы ДБО «iBank2»

Для работы с Системой ДБО «iBank2» Клиенту требуется:

1. Любой современный компьютер с операционной системой:
   - Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
   - Apple Mac OS X: 10.12 и выше;
   - Ubuntu и прочие deb-дистрибутивы (последние версии x64).
2. Web-браузер с поддержкой плагина «Bifit Signer» для использования электронной подписи с применением аппаратных криптопровайдеров. Поддержка плагина обеспечена в следующих браузерах:
   - Microsoft Edge;
   - Google Chrome;
   - Яндекс.Браузер;
   - Firefox;
   - Opera;
   - Atom;
   - Safari (совместно с Mac OS X).
3. Ключевой носитель с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. («MS_KEY K» - «АНГАРА», «Рутокен ЭЦП 2.0»).
4. Доступ в сеть Интернет для входа на сайт Системы ДБО «iBank2».
5. Подключение к сетевому или локальному принтеру, на котором будут распечатаны Сертификаты ключа проверки ЭП Клиента.
6. Наличие в компьютере пользователя USB-порта для использования ключевых носителей.
7. Наличие лицензионного, регулярно обновляемого антивирусного программного обеспечения.

Приложение 4

Требования по обеспечению информационной безопасности при работе с Системой ДБО «iBank2»

Следующие требования информационной безопасности обязательны для выполнения Клиентом:

1. Клиент должен назначить Администратора информационной безопасности - работника, ответственного за настройку безопасности эксплуатации средств защиты информации, установленных на АРМ Клиента.
2. Ключевые носители с ключами должны быть подключены к АРМ Клиента только на время работы в Системе ДБО «iBank2».
3. На АРМ Клиента должно быть установлено лицензионное антивирусное программное обеспечение и выполнена настройка автоматического обновления программного обеспечения и антивирусных баз с официального web-сайта разработчика антивирусного ПО.
4. На АРМ Клиента, при наличии, должен быть настроен персональный межсетевой экран (Firewall), имеющийся в составе операционной системы.
5. На АРМ Клиента должно использоваться лицензионное программное обеспечение (операционные системы, офисные пакеты, прикладные программы) и обеспечено автоматическое обновление системного и прикладного ПО. Не должно устанавливаться ПО с нарушением рекомендованных производителями требований.
6. Клиент обеспечивает хранение и использование Ключевого носителя таким образом, чтобы исключить доступ к нему неуполномоченных лиц. Запрещается сохранять конфиденциальную информацию в файлах (включая графические изображения) или в памяти устройств, в справочниках или «облачных» сервисах хранения информации и ресурсах в сети «Интернет». Запрещается фиксировать конфиденциальную информацию на бумажных носителях (листы для записей, распечатки документов и т.п.), доступ к которым могут получить неуполномоченные лица.
7. По окончании работы с Системой ДБО «iBank2» Ключевой носитель должен быть извлечен и хранится в месте, обеспечивающем его защиту от доступа посторонних лиц, неуполномоченных для работы в Системе. Запрещается оставлять Ключевой носитель без присмотра.
8. Для снижения риска неправомерного доступа к системе ДБО «iBank2» и информирования об ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа, клиенту Банка:
   - необходимо определить ограниченный перечень лиц имеющих доступ к системе ДБО и ЭП, правила хранения и использования носителей ЭП, перечень событий, наступление которых должно повлечь за собой немедленную замену или изъятие ключей ЭП.
   - запрещается использовать «чужие» компьютеры для доступа к Системе ДБО «iBank2», работать с Системой ДБО «iBank2» с «гостевых» рабочих мест (в интернет-кафе и т.д.) при использовании публичных сетей беспроводного доступа.
9. Не рекомендуется использовать компьютер, на котором установлено рабочее место Системы ДБО «iBank2», не по назначению, например, для игр, просмотра фильмов и т.п.
10. Производить замену ключей ЭП до истечения срока их действия во всех случаях увольнения и(или) смены полномочий и(или) лиц, имеющих доступ к Системе ДБО «iBank2» или право подписи доверенностей на получение ключей ЭП.

В целях повышения безопасности информации, обрабатываемой в Системе ДБО «iBank2»,

помимо обязательных мер, Банк рекомендует:

1. Выделить отдельную ПЭВМ, предназначенную только для работы в Системе ДБО «iBank2».
2. При отсутствии возможности использования отдельной ПЭВМ, выполнить настройку множественной загрузки ПЭВМ с созданием отдельного профиля для работы только с Системой ДБО «iBank2».
3. Установить на АРМ Клиента лицензионное специализированное программное обеспечение, повышающее уровень защищенности: межсетевой экран (Firewall), антишпионское ПО (antispyware). В настройках межсетевого экрана запретить любые соединения, кроме IP- адреса Банка.
4. Отключить неиспользуемые на АРМ Клиента сетевые протоколы и службы.
5. Отключить все общие ресурсы операционной системы, в том числе и создаваемые по умолчанию при ее установке.
6. Установить для учетной записи оператора АРМ Клиента минимальный уровень прав доступа, необходимого для нормальной работы в Системе ДБО «iBank2». Работу оператора АРМ Клиента под учетной записью с правами «администратора» исключить. Отключить стандартную учётную запись администратора, предварительно назначив административные права иной учётной записи с нестандартным именем. Установить для неё сложный пароль, отличающийся от паролей остальных учётных записей. Использовать такую учётную запись только для настройки компьютера, установки доверенного программного обеспечения и т.д.
7. Ограничить доступ работников и посторонних лиц к АРМ, используемому для работы с Системой ДБО «iBank2». Доступ к АРМ Клиента предоставить только лицам, непосредственно работающим с Системой ДБО «iBank2».
8. При использовании услуг сторонней организации или частных лиц по настройке и обслуживанию ПЭВМ, обеспечить контроль действий лица, осуществляющего непосредственную настройку и не допускать его к Системе ДБО «iBank2» и Ключам ЭП. При необходимости проверки работоспособности Системы ДБО «iBank2» она должна выполняться исключительно лицами, уполномоченными для работы с Системой.
9. Организовать хранение Ключевых носителей в персональных надежных опечатываемых хранилищах (сейфах). При использовании более одного ключа ЭП следует хранить ключи ЭП на разных ключевых носителях и использовать их для работы с Системой ДБО «iBank2» через различные устройства - это сделает невозможным отправку электронного платёжного документа вредоносной программой, заразившей одно из устройств.
10. Обеспечить использование паролей ключей ЭП, удовлетворяющих следующим минимальным требованиям:

    Пароль -

    - не должен состоять из одних цифр;
    - должен быть длиннее 8 знаков;
    - должен содержать в себе строчные и прописные буквы, цифры и знаки препинания;
    - не должен состоять из символов, находящихся на одной линии на клавиатуре;
    - не должен быть легкоугадываемым (легкоузнаваемым) значимым словом (имя, фамилия, дата рождения, девичья фамилия супруги, кличка собаки, кошки и т.д.).
11. Внимательно проверять суммы и реквизиты проводимых платежей в приходящих уведомлениях или сообщениях с Кодами подтверждения, не подтверждать подозрительные операции, и незамедлительно информировать Банк о попытках и (или) выявленных фактах мошеннических платежей.

Обращаем Ваше внимание, что выполнение указанных выше требований не сможет полностью обезопасить Вас и Ваши устройства от действий злоумышленников, но существенно поможет снизить вероятность и нежелательные последствия от таких действий.