УТВЕРЖДЕНО
Совет директоров
ООО КБ «Столичный Кредит»
Протокол от «26» июля 2022г.

Организация управления ключевыми системами электронного банкинга «iBank2» ООО КБ «Столичный кредит».

(Приложение №2 к Правилам электронного документооборота в системе электронного банкинга «iBank2» ООО КБ «Столичный кредит»).

г. Москва
2022 г.

Содержание.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет: порядок управления ключами средств криптографической защиты информации дистанционного банковского обслуживания с использованием электронного банкинга «iBank2» (ДБО) в рамках Договора обмена электронными документами с использованием системы электронного банкинга "iBank2" между Банком (ООО КБ «Столичный кредит») и Клиентом Банка и определяет требования по обеспечению информационной безопасности при работе с Системой ДБО «iBank2».

1.2. Банк обеспечивает функционирование ДБО "iBank2" с использованием программных СКЗИ Крипто-КОМ 3.4 вариант исполнения 42, 43 аппаратных СКЗИ Рутокен ЭЦП 2.0 (при их использовании клиентом).

1.3. Структурное подразделение Банка, обеспечивающее управление ключевыми системами в ДБО – группа технических средств и телекоммуникаций Отдела автоматизации Управления информационных технологий. Данное подразделение выполняет функции Центра Управления Ключевыми Системами (ЦУКС). Указанное структурное подразделение взаимодействует с Клиентами при регистрации криптографических ключей, проведении плановой замены криптографических ключей, замены криптографических ключей в случае их компрометации. Взаимодействие выполняется Банком по рабочим дням с 9.00 до 17.30 в пятницу с 9.00 до 16.15 по московскому времени (Операционное время). В случае необходимости по усмотрению Банка взаимодействие может проходить и в другое время.

1.4. Банк и Клиент (далее Стороны) признают, что используемые ими в соответствии с настоящим документом 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, в том числе имитации третьими лицами действий Клиента при использовании электронных средств платежа, при условии соблюдения Клиентом мер информационной безопасности в соответствии с Требованиями по обеспечению информационной безопасности при работе с Системой ДБО «iBank2», изложенных в разделе 7 настоящего документа. Защита ЭД от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации достигается применением: шифрования трафика между Клиентом и сервером приложений Системы ДБО «iBank2» и многофакторной аутентификацией.

1.5. Закрытые ключи электронной подписи и шифрования Клиента и соответствующие им открытые ключи электронной подписи (Пара ключей электронной подписи» (Пара ключей ЭП) – Ключ ЭП и соответствующий ему Ключ проверки ЭП) регистрируемые Банком, имеют ограниченный срок действия. Периодичность плановой смены закрытых ключей шифрования и электронной подписи устанавливается равной **1 (Один) год.**

1.6. Стороны не могут подписать электронный документ своей электронной подписью или произвести зашифрование / расшифрование информации в текущий момент времени, если к этому времени истек срок действия закрытых ключей электронной подписи или шифрования. Также Стороны не могут проверить электронную подпись электронного документа или произвести расшифрование информации в случае вывода из действия открытого ключа электронной подписи, необходимого для выполнения соответствующей операции.

1.7. Клиент не должен хранить электронные документы в архивах в зашифрованном виде. Шифрование ЭД осуществляется только для обеспечения

конфиденциальности информации при транспортировке ЭД от Клиента к Банку и в обратном направлении.

1.8. Клиент не обязан получать какую-либо дополнительную лицензию на право эксплуатации используемых в ДБО СКЗИ. При этом он обязан использовать предоставленные Банком СКЗИ только для работы в ДБО, а также обеспечивать возможность контроля использования СКЗИ со стороны Банка.

1.9. В процессе эксплуатации СКЗИ Клиент обязуется соблюдать лицензионные ограничения разработчиков СКЗИ, а также выполнять рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ (раздел 7 настоящего документа).

1.10. Владельцем открытого ключа электронной подписи в системе ДБО является физическое лицо – Клиент; физическое лицо - полномочный представитель Клиента-юридического дица. Полномочия данного лица подтверждаются учредительными документами Клиента или выданной данному лицу доверенностью, подписанной руководителем организации Клиента и заверенной печатью Клиента.

1.11. Банк обеспечивает хранение ключей электронной подписи и шифрования Клиента в электронном виде и документов на бумажном носителе – сертификатов ключа проверки электронной подписи сотрудника клиента в течение всего установленного срока хранения документов, подписанных соответствующими закрытыми ключами.

1.12. Текст настоящего документа публикуется на официальном сайте Банка по адресу www.capitalkredit.ru (далее – официальный сайт Банка) и размещается на информационных стендах в офисах Банка и может быть выдан Клиенту на бумажном носителе при личном обращении Клиента в Банк.

2. ПОРЯДОК ПОДКЛЮЧЕНИЕ К СИСТЕМЕ ДБО «IBANK2» И ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ.

Подключение Клиента к Системе ДБО «iBank2» осуществляется в следующем порядке:

При организации работы в Системе ДБО «iBank2» с использованием носителя ключа ЭП (USB –токена):

2.1. Клиент обеспечивает организацию рабочего места, отвечающего Требованиям к комплексу программно-технических средств, необходимых для работы Системы ДБО «iBank2» (Приложение №1 к настоящему документу) и в соответствии с Требованиями по обеспечению информационной безопасности при работе в Системе ДБО «iBank2» (Раздел 7 настоящего документа).

2.2. Клиент заполняет и предоставляет в Банк Заявление о подключении к системе iBank2 (Приложение №1 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2" долее Заявление) в 2 (двух) экземплярах, в котором указывает параметры подключения, фамилии, имена и отчества (при наличии) Владельцев ЭП Клиента. Владельцами ЭП Клиента, имеющими право подписи ЭД, могут быть только лица, включенные в карточку с образцами подписей и оттиска печати Клиента. Уполномоченный сотрудник Банка, принявший Заявление о присоединении, вносит отметку о дате принятия и заверяет экземпляры своей подписью.

2.3. Для сотрудников Клиента, включенных в Заявление о подключении к системе iBank2 и не имеющих право подписи ЭД, Клиент обязан предоставить в Банк Согласие на обработку персональных данных, подписанное сотрудником и заверенное руководителем/уполномоченным лицом Клиента.

2.4. В соответствии с Тарифами банка Клиент оплачивает стоимость услуг по подключению к Системе ДБО «iBank2».

2.5. На основании данных, указанных в Заявлении Банк предоставляет Клиенту требуемое количество СКЗИ (Ключевых носителей).

2.6. Клиент проходит процедуру предварительной регистрации в Системе ДБО «iBank2». Указанная процедура осуществляется Клиентом в соответствии с руководством пользователя, размещенным на сайте Банка. Во время предварительной регистрации Клиент создает необходимое количество ключей ЭП для ответственных лиц Клиента, указанных в Заявлении о присоединении Клиента. Формирование уникального идентификатора Клиента при предварительной регистрации производится в Системе ДБО «iBank2» автоматически.

2.7. Создание (генерация) Ключей ЭП в процессе предварительной регистрации осуществляется на переданных Клиенту Ключевых носителях. При этом Ключи проверки ЭП автоматически сохраняются на сервере Системы ДБО «iBank2» в Банке. В процессе генерации ключей ЭП формируется Сертификат ключа проверки электронной подписи (СКП ЭП) – электронный документ и соответствующий ему документ на бумажном носителе, заверенный подписью руководителя Клиента и оттиском печати в соответствии с указанными в карточке с образцами подписей и оттиска печати Клиента с одной стороны и Уполномоченными сотрудниками Банка с другой. Сертификат ключа проверки ЭП Клиента содержит информацию:

- о номере ключа ЭП;
- о наименовании и месте регистрации Клиента;
- о Владельце ключа ЭП (ФИО, должность, паспортные данные);
- о стандартах, требованиям которых соответствует пара ключей (ключ ЭП и ключ проверки ЭП).

2.8. Клиент распечатывает СКП ЭП (формат СКП ЭП приведен Приложении №11 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2") в двух экземплярах, проверяет правильность заполнения полей, заверяет личной подписью Владельцев ключа 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.

2.9. Срок, в течение которого СКП ЭП может быть зарегистрирован Банком, ограничен 1 (Одним) месяцем с момента его формирования. В случае предоставления в Банк СКП ЭП Клиента по истечении указанного срока такой СКП ЭП Клиента Банком не принимается.

2.10. 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 подписи в специальных полях СКП ЭП и заверяют штампами и печатями Банка, определенными для этих целей. Один экземпляр СКП ЭП остается в Банке, второй передается Клиенту. При каждой регистрации новых Ключей ЭП в Системе ДБО «iBank2» уполномоченный сотрудник Банка, принимающий от Клиента распечатанный СКП ЭП, проверяет документы, подтверждающие полномочия Владельцев ключей ЭП. После успешной проверки, производится окончательная регистрация Клиента в Системе ДБО «iBank2», активируются ключи Владельцев ключей ЭП Клиента. День регистрации является датой начала работы Клиента в Системе ДБО «iBank2». 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(ей) ЭП и предоставить необходимые документы.

При организации работы в Системе ДБО «iBank2» с использованием электронной ЭП в облаке:

2.11. Клиент обеспечивает организацию рабочего места, отвечающего Требованиям к комплексу программно-технических средств, необходимых для работы Системы ДБО «iBank2» (Приложение №1 к настоящему документу) и в соответствии с Требованиями по обеспечению информационной безопасности при работе в Системе ДБО «iBank2» (Раздел 7 настоящего документа).

2.12. Клиент заполняет и предоставляет в Банк Заявление о подключении к системе iBank2 (Приложение №1 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2" далее Заявление) в 2 (двух) экземплярах, в котором указывает параметры подключения, фамилии, имена и отчества (при наличии) Владельцев ЭП Клиента. Владельцами ЭП Клиента, имеющими право подписи ЭД, могут быть только лица, включенные в карточку с образцами подписей и оттиска печати Клиента. Уполномоченный сотрудник Банка, принявший Заявление о присоединении, вносит отметку о дате принятия и заверяет экземпляры своей подписью.

2.13. Для сотрудников Клиента, включенных в Заявление о подключении к системе iBank2 и не имеющих право подписи ЭД, Клиент обязан предоставить в Банк Согласие на обработку персональных данных, подписанное сотрудником и заверенное руководителем/уполномоченным лицом Клиента.

2.14. В соответствии с Тарифами банка Клиент оплачивает стоимость услуг по подключению к Системе ДБО «iBank2».

2.15. Клиент (сотрудник клиента) осуществляет самостоятельную предварительную регистрацию через Интернет с помощью АРМ «Интернет-Банк для бизнеса» (далее – Интернет-Банк), на этом этапе:

- выбирается тип электронной подписи, которую планируется создать (облачная ЭП);

- вводится информация об организационной форме организации клиента, реквизиты организации (ИНН (КИО), КПП, ОГРН, адрес организации на русском языке);

- вводятся номера счетов организации;

- вводится информация о контактном лице (ФИО, номер телефона), блокировочное слово (для подтверждения подлинности);

- вводится информация о владельце ключа ЭП (ФИО владельца, должность, данные документа, удостоверяющего личность, номер телефона и адрес электронной почты);

- вводится информация о выдаче доверенности Банку на хранение ключа ЭП (в защищенном хранилище и использовании его для формирования ЭП под документами Системы ДБО «iBank2»);

- задается название электронной подписи и пароль.

2.16. Клиент (сотрудник клиента) после успешной предварительной регистрации формирует в автоматическом режиме Сертификат ключа проверки электронной подписи (СКП ЭП) содержащий информацию:

- о номере ключа ЭП;
- о наименовании и месте регистрации Клиента;

- о Владельце ключа ЭП (ФИО, должность, паспортные данные);
- о стандартах, требованиям которых соответствует пара ключей (ключ ЭП и ключ проверки ЭП).

2.17. Клиент распечатывает СКП ЭП (формат СКП ЭП приведен в Приложении №11 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2") в трехэкземплярах, проверяет правильность заполнения полей, заверяет личной подписью Владельцев ключа 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. Три экземпляра СКП ЭП передаются в Банк для проверки и регистрации.

2.18. Срок, в течение которого СКП ЭП может быть зарегистрирован Банком, ограничен 1 (Одним) месяцем с момента его формирования. В случае предоставления в Банк СКП ЭП Клиента по истечении указанного срока такой СКП ЭП Клиента Банком не принимается.

2.19. 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 подписи в специальных полях СКП ЭП и заверяют штампами и печатями Банка, определенными для этих целей. Один экземпляр СКП ЭП остается в Банке, второй передается Клиенту. При каждой регистрации новых Ключей ЭП в Системе ДБО «iBank2» уполномоченный сотрудник Банка, принимающий от Клиента распечатанный СКП ЭП, проверяет документы, подтверждающие полномочия Владельцев ключей ЭП. После успешной проверки, производится окончательная регистрация Клиента в Системе ДБО «iBank2», активируются ключи Владельцев ключей ЭП Клиента. День регистрации является датой начала работы Клиента в Системе ДБО «iBank2». 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(ей) ЭП и предоставить необходимые документы.

2.20. При подключении к системе ДБО «iBank2» с использованием **ЭП в облаке** Клиент доверяет Банку хранить ключ ЭП в защищенном хранилище и использовать его для формирования ЭП под документами системы «iBank2».

2.21. В случае подписания запроса на новый ключ сотрудника Клиента действующей ЭП того же сотрудника Клиента, Клиент может самостоятельно выпустить облачную ЭП без визита в Банк и без предоставления заверенных запросов на бумажном носителе.

По желанию клиента он может распечатать сертификат проверки ключа ЭП на бумажном носителе в трех экземплярах и предоставит его в Банк для заверения, один экземпляр передается обратно клиенту, два других остаются в Банке и прикладываются к досье клиента соответствующих подразделений.

3. СРОК ДЕЙСТВИЯ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ. СМЕНА КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

3.1. Максимальный срок действия Ключа ЭП и СКП ЭП не может превышать **1 (Одного) года** со дня регистрации СКП ЭП Клиента в Системе ДБО «iBank2». По окончании срока действия Ключа ЭП работа Клиента с данным ключом блокируется

3.2. В Системе ДБО «iBank2» осуществляется контроль сроков полномочий Владельцев ключей ЭП. Срок полномочий Владельца ключа ЭП Клиента определяется на

основании учредительных, организационно-распорядительных (приказов, трудовых договоров, протоколов заседаний органов управления, доверенностей) и иных документов, находящихся в Юридическом деле Клиента. После истечения срока полномочий Владельца ключа ЭП, если Клиент не предоставил в Банк документы, подтверждающие продление полномочий Владельца ключа ЭП, работа с Ключом ЭП данного Владельца блокируется.

3.3. Банк с использованием Системы ДБО «iBank2» уведомляет Владельца ключа ЭП о предстоящем истечении срока действия Ключа ЭП или срока полномочий Владельца ключа ЭП за 30 календарных дней до даты окончания срока. При входе в систему Владелец ключа ЭП получает уведомление с информацией о количестве дней, когда закончится срок действия его полномочий или срок действия Ключа ЭП и предложением предоставить в банк документы, подтверждающие продление полномочий, или сгенерировать новый Ключ ЭП. Рекомендуется осуществлять генерацию нового Ключа ЭП взамен действующего в срок не позднее, чем за 10 (десять) календарных дней до даты окончания срока действия активного Ключа ЭП.

3.4. Генерация новых Ключей ЭП может быть осуществлена в соответствии с пунктами 2.6-2.8, 2.15 настоящего документа средствами Системы ДБО «iBank2».

3.5. Владельцы ключей ЭП Клиента имеют возможность генерировать для себя новые ключи ЭП без посещения Банка для регистрации СКП ЭП. Создание ключей ЭП при этом осуществляется в разделе «Ключи ЭП» Системы ДБО «iBank2». Условиями для дистанционного выпуска СКП ЭП являются:

- активный статус Владельца ключа ЭП в Системе ДБО «iBank2»;
- актуальность реквизитов документа, удостоверяющего личность Владельца ключа ЭП.

3.6. Внеплановая смена Ключей ЭП осуществляется в следующих случаях:

- при компрометации Ключа ЭП;
- при изменении следующих сведений о Клиенте:
  - - организационно-правовая форма собственности Клиента;
  - - ИНН или ОГРН Клиента;
  - - фамилия, имя, отчество и данные, идентифицирующие Владельца ключа ЭП, содержащиеся в документах, предоставленных Банку;
- при изменении Владельцев ключей ЭП, уполномоченных Клиентом заверять ЭД в Системе ДБО «iBank2» электронной подписью;
- при повреждении ключевого носителя;
- в иных случаях невозможности пользования имеющимися Ключами ЭП.

3.7. В случаях, перечисленных в п. 3.6 настоящего документа, Банк приостанавливает электронный документооборот с Клиентом до регистрации в Системе ДБО «iBank2» нового СКП ЭП. Клиент осуществляет генерацию новых Ключей ЭП с последующей передачей в Банк новых СКП ЭП. Запись новых Ключей ЭП после их генерации может осуществляться на носитель ключей ЭП (в случае использования USB – токена), либо храниться в защищенном хранилище Банка (облаке). При повреждении (утере) ключевого носителя, используемого Клиентом, Клиент может обратится в Банк за получением нового Ключевого носителя. При наличии в Банке на момент обращения Клиента, Ключевых носителей, предоставление их Клиенту осуществляется за плату в соответствии с тарифами Банка. Ключ, содержавшийся на утерянном токене, при этом блокируется, на новый токен выпускается новый ключ.

3.8. Внеплановая смена ключей осуществляется в соответствии с пунктами 2.6-2.8, 2.15 настоящего документа.

4. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ.

4.1. К событиям, на основании которых лицо, владеющее закрытым ключом электронной подписи и/или шифрования, принимает решение о его компрометации, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключам;
- возникновение подозрений на утечку информации или ее искажение в СЭД;
- совершении попыток неправомерного получения персональной информации пользователей систем ДБО
- наличие хакерских, вирусных или иных атак, которые могут являться попытками осуществить хищение ключей ЭП.
- нарушение правил хранения ключевых носителей.

4.2. В случае компрометации Ключей ЭП, Средств доступа или подозрении на их компрометацию, в том числе утраты носителя(ей) Ключа ЭП и (или) наличия информации о его использовании без согласия Клиента, возникновении любых подозрений на компрометацию среды исполнения (наличие в компьютере вредоносных программ, нестандартная работа системного программного обеспечения и т.д.), Клиент обязан незамедлительно направить в Банк уведомление о компрометации по электронной почте info@capitalkredit.ru или по факсу (495) 229-00-50 (1231), (495) 795-07-61 с указанием номера телефона лица Клиента и сообщить об этом в Банк по телефонам (495) 229-00-50 или (495) 795-07-60. Обработка уведомлений сотрудниками Банка производится в Операционное время. Уведомления, поступившие после Операционного времени, обрабатываются на следующий рабочий день.

4.3. При получении Банком информации о компрометации Ключа ЭП Банк незамедлительно приостанавливает работу Клиента в Системе ДБО «iBank2». Одновременно Банк сообщает Клиенту о приостановлении работы Клиента в Системе ДБО «iBank2» в связи с получением информации о компрометации Ключей ЭП, Средств доступа или среды исполнения. Способ информирования Клиента о приостановлении работы Клиента в Системе ДБО «iBank2» в связи с компрометацией Ключа ЭП определяется Банком самостоятельно. До получения от Клиента в письменном виде подтверждения или опровержения факта компрометации Ключа ЭП прием документов Клиента осуществляется только на бумажном носителе.

4.4. Не позднее следующего рабочего дня после уведомления Банка о компрометации Клиент обязан предоставить в Банк в письменной форме Заявление об аннулировании СКП ЭП по форме Приложения №3 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2". Копия заявления с отметкой сотрудника Банка о дате и времени приема заявления возвращается Клиенту. В случае непредставления Клиентом Заявления об аннулировании СКП ЭП в течение 10 рабочих дней, Ключ ЭП удаляется из списка Ключей ЭП Клиента.

4.5. В случае невыполнения Клиентом обязанностей, предусмотренных п.6.1 и п.6.3. настоящего Порядка, Банк не несет ответственности за возможные финансовые потери Клиента, связанные с незаконным использованием Системы ДБО «iBank2» неуполномоченными лицами.

4.6. При получении от Клиента уведомления, предусмотренного п.4.4 настоящего документа, после осуществления списания денежных средств с Банковского счета Клиента,

Банк обязан незамедлительно направить оператору по переводу денежных средств, обслуживающему получателя средств, уведомление о приостановлении зачисления денежных средств на банковский счет получателя средств.

4.7. Открытый ключ электронной подписи, соответствующий скомпрометированным закрытым ключам, исключается из ключевой базы Банка и хранится в течение срока хранения документов, подписанных скомпрометированным закрытым ключем электронной подписи для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

5. АННУЛИРОВАНИЕ ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Банк аннулирует открытый ключ электронной подписи Клиента в следующих случаях:

- после осуществления плановой смены криптографических ключей;
- в случае прекращения действия Договора обмена электронными документами с использованием системы электронного банкинга "iBank2";
- по заявлению в письменной форме Клиента, подписанного руководителем Клиента и заверенного печатью Клиента

5.2. В случае аннулирования открытого ключа электронной подписи Клиента Банк исключает его справочника открытых ключей электронной подписи открытый ключ хранится в течение срока хранения документов, подписанных аннулируемым закрытым ключом электронной подписи для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением электронной подписи.

5.3. Дата и время, с которого открытый ключ электронной подписи считается недействительным, устанавливается равным времени наступления обстоятельств, перечисленных в п. 5.1.

6. РАЗРЕШЕНИЕ СПОРОВ. ПОРЯДОК ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ ПРИ РАЗРЕШЕНИИ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. 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. Срок ответа на претензию – 30 (тридцать) календарных дней с момента ее получения, если иной срок не установлен настоящим Порядком.

6.2. Разногласия, по которым Сторонами не достигнуты договоренности, подлежат рассмотрению судом в соответствии с законодательством Российской Федерации.

6.3. Приостановление использования Системы ДБО «iBank2», а также временное прекращение осуществления Операций в Системе ДБО «iBank2» по инициативе одной из Сторон не влечет прекращения обязательств по взаиморасчетам и возмещению убытков, возникших до момента приостановления использования Системы ДБО «iBank2» или прекращения осуществления Операций.

6.4. При несогласии со списанием денежных средств по Операции, проведенной с использованием Системы ДБО «iBank2», Клиент обязан направить в Банк заявление в письменной форме о совершении спорной Операции, путем официального вручения под расписку ответственному исполнителю Банка. Заявление направляется не позднее рабочего

дня, следующего за днем получения от Банка уведомления о совершенной Операции. В заявлении необходимо указать:

- тип Операции (списание денежных средств или пополнение, или иное);
- дата и время совершения Операции;
- сумма операции и валюта Операции;
- известные Клиенту сведения об обстоятельствах утраты ключа ЭП и (или) неправомерном его использовании (если выявлены факты компрометации Ключа ЭП);
- тип операционной системы, антивирусное программное обеспечение, IP-адреса, используемые Клиентом.

6.5. Банк обязан рассмотреть заявление о несогласии со списанием денежных средств по Операции в срок до 30 (тридцати) календарных дней (в случае осуществления трансграничного перевода денежных средств – в срок до 60 (шестидесяти) календарных дней) с даты получения такого заявления.

6.6. Для рассмотрения заявления, связанного с оспариванием Операции, проведенной с использованием Системы ДБО «iBank2», может быть сформирована экспертная комиссия.

6.7. Порядок создания и работы экспертной комиссии описан в Приложении №2 к Договору обмена электронными документами с использованием системы электронного банкинга "iBank2"

6.8. В случае несогласия одной из Сторон с решением экспертной комиссии, отказе одной из Сторон исполнять рекомендации комиссии или отказе одной из Сторон разрешать споры и разногласия в порядке, установленном в настоящем разделе документа, несогласная Сторона обращается в Арбитражный суд города Москвы в порядке, установленном действующим законодательством Российской Федерации.

7. РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ.

7.1. Режим эксплуатации СКЗИ, применяемых в ДБО, устанавливается в соответствии с "Требованиями к средствам криптографической защиты конфиденциальной информации" по уровню "КС1".

7.1.1. Рекомендации по организационному обеспечению безопасности СКЗИ:

- в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ;
- в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;
- к работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

7.1.2. Рекомендации по размещению СКЗИ и режиму охраны:

- помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;

- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СКЗИ оборудуются средствами контроля вскрытия;
- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ.

7.1.3. Рекомендации по обеспечению безопасности ключевой информации (в случае использования ключевых носителей (USB –токена) :

- ключевые носители с закрытыми ключами электронной подписи и шифрования и инсталляционные дискеты с программным обеспечением СКЗИ в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение закрытых ключей поручается руководством организации Клиента специально выделенным сотрудникам;
- для хранения ключевых носителей с закрытыми ключами электронной подписи и шифрования выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключей и инсталляционных дискет с программным обеспечением СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение;
- при транспортировке ключевых носителей с закрытой ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

7.2. В целях обеспечения безопасной работы Клиенту рекомендуется соблюдать Требования по обеспечению информационной безопасности при работе в Системе ДБО «iBank2» (Приложение №2 к настоящему документу).

Приложение №1 к

Организации управления ключевыми системами
электронного банкинга «iBank2» ООО КБ «Столичный кредит»

Требования
к комплексу программно-технических средств необходимых для работы
Системы ДБО «iBank2» ООО КБ «Столичный кредит»

Для работы с Системой ДБО «iBank» 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: 10.6 (Snow Leopard) и выше;
   - Linux: AltLinux 7 (x86/x64), Debian 7 (x86/x64), Mint 13 (x86/x64), SUSE Linux Enterprise Desktop 12 (x64), openSUSE 13 (x86/x64), Ubuntu 12.04 (x86/x64) и более современные версии указанных дистрибутивов.

2. Web-браузер с поддержкой плагина «Bifit Signer» для использования электронной подписи с применением аппаратных криптопровайдеров. Поддержка плагина обеспечена в следующих браузерах:

   - Internet Explorer версия 11;
   - Firefox (последняя);
   - Opera (последняя);
   - Safari (последняя);
   - Chrome (последняя).

3. Ключевой носитель с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. («Рутокен ЭЦП 2.0»). (данная опция необходима в случае использования аппаратного ключевого носителя).

4. Доступ в сеть Интернет для входа на сайт Системы ДБО.

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 (данная опция необходима в случае использования аппаратного ключевого носителя).
7. Наличие лицензионного, регулярно обновляемого антивирусного программного обеспечения.

Приложение № 2 к

Организации управления ключевыми системами
электронного банкинга «iBank2» ООО КБ «Столичный кредит»

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

I. Следующие требования информационной безопасности обязательны для выполнения Клиентом в случае использования для работы с системой ДБО «iBank2» Ключевого носителя:

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 (в случае работы с ними) 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 должны быть отключены сервисы, позволяющие удаленно управлять компьютером.
6. 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.
7. 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.
8. 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.
9. Запрещается использовать «чужие» компьютеры или мобильные устройства 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.
10. Не рекомендуется использовать компьютер, на котором установлено рабочее место Системы ДБО «iBank2», не по назначению, например, для игр, просмотра фильмов и т.п.
11. 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:

- Выделить отдельную ПЭВМ, предназначенную только для работы в Системе ДБО «iBank2».
- При отсутствии возможности использования отдельной ПЭВМ, выполнить настройку множественной загрузки ПЭВМ с созданием отдельного профиля для работы только с Системой ДБО «iBank2».
- 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.
- Отключить неиспользуемые на АРМ Клиента сетевые протоколы и службы.
- Отключить все общие ресурсы операционной системы, в том числе и создаваемые по умолчанию при ее установке.
- 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.

- 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».
- 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.
- Использовать услугу фильтрации IP-адресов.
- Использовать услугу дополнительного подтверждения платежных поручений с помощью Кодов подтверждения в SMS- сообщениях.
- 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.
- 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.).

- 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.

II. Следующие требования информационной безопасности обязательны для выполнения Клиентом в случае использования для работы с системой ДБО «iBank2» электронной подписи в облаке:

1. Клиент должен назначить Администратора информационной безопасности – работника, ответственного за настройку безопасности эксплуатации средств защиты информации, установленных на АРМ Клиента.
2. На устройстве (персональный компьютер, ноутбук, смартфон, планшет) Клиента с которого осуществляется доступ в систему ДБО «iBank2» (далее по тексту настоящей части – устройство) должно быть установлено лицензионное антивирусное программное обеспечение и выполнена настройка автоматического обновления программного обеспечения и антивирусных баз с официального web-сайта разработчика антивирусного ПО.
3. На устройстве Клиента должно использоваться лицензионное программное обеспечение (операционные системы, офисные пакеты, прикладные программы) и обеспечено автоматическое обновление системного и прикладного ПО. Клиент должен обеспечить: инфраструктуру безопасного доступа к сервису облачной ЭП, защиту от утечек данных, защиту информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.
4. Клиент должен 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.
5. 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.
6. Ограничить доступ работников и посторонних лиц к устройствам, используемым для работы с Системой ДБО «iBank2». Доступ к АРМ Клиента предоставить только лицам, непосредственно работающим с Системой ДБО «iBank2».
7. 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.

8. Использовать услугу дополнительного подтверждения платежных поручений с помощью Кодов подтверждения в SMS- сообщениях. Использовать услугу фильтрации IP-адресов.

9. 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.

Клиент должен осознавать, что гарантировать информационную безопасность использования ЭП может только доверенная среда (изолированная), в которой клиент и технические средства в момент взаимодействия защищены от посторонних вмешательств. 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.