УТВЕРЖДЕНЫ
Правлением АО «МОСКОМБАНК»
Протокол № 01-05/33 от 24.07.2024
Введены в действие с 25.07.2024
Приказом № 01-08/59 от 24.07.2024

МОСКОМБАНК
Commercial Bank of Moscow

ПРАВИЛА
дистанционного банковского обслуживания
АО «МОСКОМБАНК»
для корпоративных клиентов

(версия 9.0)

Москва
2024

ОГЛАВЛЕНИЕ

1. ОПРЕДЕЛЕНИЯ

Перечень терминов и определений, указанных в настоящем разделе Правил, не является исчерпывающим. Другие пункты Правил, заявлений, дополнений и приложений к ним могут устанавливать дополнительные определения.

Банк – АО «МОСКОМБАНК».

Клиент – корпоративный клиент (юридическое лицо или индивидуальный предприниматель, физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой).

Сторона, Стороны – Банк и/или Клиент.

Счет – банковский счет Клиента, открываемый Банком на имя Клиента на основании договора банковского счета.

Система – «iBank2» - электронное средство платежа, позволяющее Клиенту составлять, удостоверять и передавать в Банк распоряжения в целях осуществления перевода денежных средств с использованием информационно-телекоммуникационных технологий, а также средство электронного документооборота, технически представляющее из себя совокупность программно-аппаратных средств и используемых на стороне Клиента и Банка. Уполномоченным Банком разработчиком Системы «iBank2» является АО «БИФИТ» (г. Москва, ИНН 7719617469).

ДБО (Дистанционное банковское обслуживание) – технологии и процедуры, проводимые Клиентом и Банком с целью дистанционного обслуживания в Системе.

Правила – настоящие «Правила дистанционного банковского обслуживания АО «МОСКОМБАНК» для корпоративных клиентов».

Заявление – Заявление на дистанционное банковское обслуживание, направляемое Клиентом Банку.

Договор – договор о дистанционном банковском обслуживании, образованный Правилами, являющимися публичной офертой Банка, акцептованные Клиентом, посредством должным образом подписанного и оформленного Заявления.

Электронный документ (ЭД) – совокупность информации в цифровой форме, содержащая финансовый документ, нефинансовый документ, информационное или служебное сообщение в Системе.

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.

Простой электронной подписью (ПЭП) является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. ПЭП состоит из уникальной последовательности символов, сформированной с использованием аутентификационных данных Клиента (уполномоченного лица), атрибутов подписываемого документа, а также времени создания подписи. Ключом ПЭП является код подтверждения, полученный от Клиента (уполномоченного лица) при аутентификации в Системе, созданный на основе логина и пароля. Клиент (уполномоченное лицо) обязан соблюдать конфиденциальность ключа ПЭП, не передавать его третьим лицам, и незамедлительно уведомлять в Банк в случае его компрометации.

Усиленной неквалифицированной электронной подписью (УНЭП/НЭП) является электронная подпись, которая:

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

Ключ ЭП Клиента – ключ (уникальная последовательность символов), самостоятельно генерируемый Клиентом с использованием средств Системы, и предназначенный для создания Клиентом ЭП электронных документов.

Ключ проверки ЭП Клиента – ключ (уникальная последовательность символов, однозначно связанная с ключом ЭП Клиента), самостоятельно генерируемый Клиентом с использованием средств Системы, и предназначенный для проверки Банком подлинности ЭП электронного документа, сформированного Клиентом.

Владелец ЭП – лицо, имеющее право распоряжения денежными средствами на счетах Клиента, которому в соответствии с законодательством Российской Федерации и Правилами выдан Сертификат ключа проверки ЭП Клиента. К владельцам ЭП может быть отнесено физическое лицо, на имя которого Клиентом составлен Сертификат ключа проверки ЭП Клиента, и которое владеет соответствующим ключом на основании доверенности или иного распорядительного акта Клиента.

Подлинная электронная подпись – электронная подпись электронного документа, проверка которой с использованием соответствующего ключа проверки ЭП дает положительный результат.

Сертификат ключа проверки ЭП Клиента – бумажный или электронный документ с представленным в шестнадцатеричном виде ключом проверки ЭП Клиента, датой начала и окончания действия ключа ЭП Клиента, заверенный подписями (в том числе ЭП) уполномоченных лиц Клиента и оттиском печати Клиента в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке, и подтверждающий принадлежность Ключа проверки ЭП Клиента Владельцу ЭП.

Активный ключ ЭП Клиента – ключ ЭП Клиента, зарегистрированный Банком в Системе, и используемый Клиентом для работы в Системе.

Средство криптографической защиты информации (СКЗИ) – СКЗИ Крипто-КОМ версии 3.4 компании ЗАО «Сигнал-КОМ», входящее в состав Системы и имеющее сертификаты ФСБ России СФ/114-3268, СФ/124-3269 от 11.01.2018, удостоверяющие, что СКЗИ соответствует требованиям российских государственных стандартов в области криптографической защиты, требованиям ФСБ России к стойкости СКЗИ и может, соответственно, использоваться для обеспечения безопасности информации уровня КС1 и КС2, не содержащей сведений, составляющих государственную тайну.

USB-токен - аппаратное USB-устройство, в которой реализованы российские криптоалгоритмы и имеется защищенная область памяти, позволяющее генерировать и безопасно хранить ключи ЭП.

MAC-токен – аппаратное устройство, вычисляющее ЭП Клиента с использованием реквизитов платежа. Может использоваться при подтверждении платежного документа, подтверждения платежей свыше установленного лимита и управления списками доверенных получателей платежей Клиента. Использование реквизитов платежа при формировании цифрового кода данным устройством позволяет повысить безопасность использования Системы.

SMS-аутентификация и SMS – сообщение службы коротких сообщений (SMS), направляемое Клиенту Банком на его устройство (телефон) подвижной радиотелефонной связи, содержащее одноразовый пароль для целей подтверждения платежного документа или аутентификации в Системе.

IP-фильтрация - фильтрация IP адресов, позволяющая осуществлять вход в Систему только с определенных компьютеров. Используется для повышения информационной безопасности при работе в системе ДБО в случае, если Клиент работает со счетом постоянно с одних и тех же рабочих мест.

Центр «ЛСЗ» ФСБ России – Центр по лицензированию, сертификации и защите государственной тайны ФСБ России.

Блокировочное слово – пароль, определяемый Клиентом при регистрации в Системе. Блокировочное слово может быть использовано Клиентом (например, в случае Компрометации ключа) для блокирования своей работы в Системе по телефонному звонку в Банк.

Компрометация ключа – утрата, хищение, несанкционированное копирование, передача закрытого ключа в линию связи в открытом виде, любые другие виды разглашения содержания

ключа, а также случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

Подлинность электронного документа означает, что данный документ создан в Системе без отступлений от принятой технологии.

Целостность электронного документа означает, что после его создания и заверения электронной подписью в его содержание не вносилось никаких изменений.

Авторство электронного документа – это свидетельство того, что электронный документ создан и подписан уполномоченными лицами участника Системы.

Экспертная комиссия — комиссия из уполномоченных представителей Сторон, создаваемая Сторонами в целях разрешения разногласий в случае оспаривания факта направления / получения ЭД и/или проставления ЭП на ЭД и/или подлинности ЭП на ЭД.

Вредоносный код (далее – ВК, вирус) - компьютерная программа, предназначенная для внедрения в автоматизированные системы, ПО, средства вычислительной техники, телекоммуникационное оборудование пользователей Системы, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации (в том числе защищаемой в соответствии с действующим законодательством), а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Услуги – дополнительные услуги Банка и/или его партнеров, которые предоставляются в электронной форме с использованием Системы.

Тарифы – «Услуги и тарифы для корпоративных клиентов (юридических лиц, индивидуальных предпринимателей и лиц, занимающихся частной практикой) АО «МОСКОМБАНК».

Сайт Банка – официальный сайт Банка в сети Интернет: *москомбанк.рф (https://moscombank.ru).*

Опубликование информации - размещение Банком информации в местах и способами, установленными Правилами, обеспечивающими возможность ознакомления с этой информацией Клиентов. Опубликование информации не означает ее обязательного распространения через средства массовой информации.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила определяют порядок предоставления Банком ДБО, который позволяет Клиентам получать дистанционный доступ к Счетам, передавать электронные расчетные документы, принимать выписки по Счетам, передавать и принимать нефинансовые документы, информационные и сервисные сообщения, а также подключать и отключать Услуги.

2.2. ДБО предоставляется только Клиентам, в отношении которых полностью завершены процедуры идентификации и с которыми заключен договор банковского счета.

2.2.1 Заключение Договора между Банком и Клиентом осуществляется путем присоединения Клиента к изложенным в Правилах условиям в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Направляя в Банк Заявление (по форме Приложения № 1 к Правилам), Клиент заявляет о своем присоединении в полном объеме к Правилам. Договор считается заключенным между Сторонами с момента, указанного в пункте 10.1 Правил.

2.2.2. Клиент может выбрать следующие варианты использования ЭП:

- авторизация и подписание электронных документов УНЭП с использованием USB-токена и/или MAC-токена;
- авторизация и подтверждение ЭД ПЭП с применением SMS-аутентификации.

2.2.3. По заявлению Клиента (Приложение № 6 к Правилам) некоторые договоры банковского счета, заключенные между Банком и Клиентом, могут быть исключены из общего правила, указанного в п. 2.2 Правил.

2.3. Клиент подтверждает, что до присоединения к Правилам ознакомился и проинформирован об условиях использования ДБО, в частности о любых ограничениях способов и мест использования, случаях повышенного риска его использования как электронного средства платежа.

2.4. Банк предоставляет Клиенту следующие услуги с использованием Системы на платной основе, если такая плата установлена Тарифами Банка:

- прием от Клиента ЭД на выполнение операций по Счетам;
- предоставление Клиенту в форме ЭД информации об операциях, совершенных по Счетам Клиента;
- прием от Клиента и предоставление Клиенту ЭД, предусмотренных законодательством, в том числе в области валютного регулирования и валютного контроля;
- прием от Клиента и предоставление Клиенту ЭД в соответствии с договорами, заключенными между Клиентом и Банком;
- прием от Клиента и предоставление Клиенту ЭД свободного формата;
- подключение к Системе с фиксированных IP-адресов;
- подключение и отключение Услуг.

2.5. Банк с целью ознакомления Клиентов с Правилами, изменениями и дополнениями к ним, Тарифами, изменениями и дополнениями к ним, а также изменениями своего места нахождения, банковских и иных реквизитов размещает их путём Опубликования информации одним или несколькими из указанных способов:

- размещение информации в местах обслуживания Клиентов;
- размещение информации на Сайте;
- оповещение Клиентов средствами ДБО;
- иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

2.6. Датой доведения до сведения Клиента Правил, Тарифов и изменений и/или дополнений к ним считается дата направления Банком Клиенту соответствующего уведомления или дата Опубликования информации.

2.6.1. Информация, переданная Банком Клиенту с использованием ДБО, считается доведённой до сведения Клиента по истечении 1 (одного) дня с момента её передачи Клиенту, независимо от фактического восприятия информации Клиентом (независимо от того, прочитана информация или нет).

2.6.2. Клиент не вправе ссылаться на незнание указанной информации при неисполнении или ненадлежащем исполнении своих обязательств по Договору, в том числе при предъявлении жалоб/претензий Банку и разрешении возникших споров с Банком.

2.7. Заключая Договор, Банк и Клиент принимают на себя обязательство исполнять в полном объеме требования Правил и Тарифов.

2.8. Если в тексте Правил явно не оговорено иное, предполагается, что уведомления, требования и иная корреспонденция (далее – корреспонденция), направляемая Банком Клиенту на бумажном носителе, направляется по адресу Клиента, имеющемуся в Банке. Указанная корреспонденция будет считаться отправленной Клиенту по надлежащему адресу, если Клиент ранее не уведомил Банк о его изменении.

2.9. Изменения/дополнения Правил считаются принятыми Клиентом, если Клиент с даты доведения до сведения Клиента указанной информации, определяемой согласно пункту 2.5 Правил, продолжает пользоваться ДБО, в том числе совершает операции, исполняет обязанности и осуществляет права по Договору, обращается в Банк, в том числе по телефону, с использованием Интернета или по ДБО по вопросам, связанным с использованием ДБО, за исключением представления заявления о расторжении Договора.

2.10. Любые изменения/дополнения Правил с даты их вступления в силу равно распространяются на всех лиц, присоединившихся к Правилам, в том числе присоединившихся к Правилам ранее дня вступления изменений/дополнений в силу, с учётом положений настоящего раздела Правил.

3. ДОКУМЕНТЫ

3.1. Стороны договорились использовать в электронной форме любые документы, предусмотренные законодательством Российской Федерации, нормативными актами Банка России и Банка (платежные поручения, заявления на перевод иностранной валюты, поручения на покуп-

ку/продажу/конвертацию иностранной валюты, распоряжения на списание иностранной валюты с транзитного счета, ведомости к платежным документам, выписки по Счетам), запросы, письма, уточнения, отзывы, уведомления, заявления на подключение или отключение Услуг, а также иные документы, не являющиеся платежными, составленные в свободном формате, в том числе документы валютного контроля (заявления о постановке на учет контракта (кредитного договора), заявления о внесении изменений в раздел I ведомости банковского контроля, заявления о снятии с учета контракта (кредитного договора), сведения о валютных операциях, справки о подтверждающих документах и т.п.), документы, используемые в процессе реализации факторинговых или кредитных сделок, иные документы Клиента и Банка.

3.2. По требованию Банка Клиент обязан в двухдневный срок предоставить на бумажном носителе экземпляр любого ЭД, указанного в п.3.1 Правил, подписанного уполномоченными лицами и заверенного оттиском печати Клиента, в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке.

3.3. ЭД, указанные в п.3.1 Правил, изготавливаются на основе использования предоставляемого Банком программного обеспечения Системы. Форматы ЭД формируются Системой на основании требований законодательства Российской Федерации и правил Банка.

3.3.1. Если программное обеспечение Системы не предусматривает создание ЭД, то он может быть создан Клиентом с использование иного программного обеспечения. В таком случае ЭД направляется в Банк в виде прикрепленного файла к письму.

3.4. Перечень реквизитов платежных ЭД должен соответствовать реквизитам соответствующего расчетного документа, форма (формат) которого установлена законодательством Российской Федерации и правилами Банка.

3.5. Подлинником ЭД является электронный образ документа в оговоренном формате, который содержит текст документа и ЭП уполномоченных (-ого) лиц (а) Стороны, подписавшей этот документ, с положительным результатом проверки подлинности ЭП, произведенной программными средствами Системы, с использованием ключей проверки ЭП, зарегистрированных в установленном Правилами порядке. Результаты проверки подлинности фиксируются с использованием средств Системы.

3.6. Если ЭД содержит в себе другой вложенный ЭД (например, письмо, созданное средствами Системы, содержит в себе прикрепленный сканированный документ Клиента и т.п.), то ЭП, проставленная на первом ЭД, считается проставленной и на другой вложенный ЭД.

4. УСЛУГИ

4.1. Банк предоставляет возможность Клиенту с использованием Системы подключать, получать и отключать Услуги.

4.2. Состав Услуг определяется Банком и может быть изменен им в одностороннем порядке и без предварительного уведомления.

4.3. Услуги предоставляются на условиях Правил, а также приложений к ним, в которых могут быть установлены дополнительные условия предоставления тех или иных Услуг, непротиворечащие Правилам.

4.4. За предоставление Услуг Банк взимает комиссию в объеме и в порядке, предусмотренном в Тарифах.

4.5. После заключения Договора, Клиенту необходимо зарегистрироваться в Системе.

4.5.1. В случае, если Клиент предполагает использовать ПЭП, регистрация осуществляется сотрудником Банка, после чего Клиенту автоматически направляется сообщение по адресу электронной почты, который Клиент указал в Заявлении на подключение ДБО. Сообщение содержит ссылку, по которой открывается окно для ввода одноразового пароля, направленного Клиенту СМС-сообщением на мобильный телефон, указанный в Заявлении на подключение ДБО. Клиент вводит одноразовый пароль в открывшемся окне и далее устанавливает постоянный пароль, который будет в дальнейшем использоваться в Системе совместно с одноразовым паролем, направляемым SMS-сообщением.

4.5.2. В случае, если Клиент предполагает использовать УНЭП, то регистрация проходит в нижеследующем порядке.
4.5.2.1. Клиенту необходимо предварительно установить драйвер USB-токена; подключить USB-токен к USB порту компьютера; в качестве хранилища ключей выбрать из списка USB-токен.
4.5.2.2. Предварительная регистрация осуществляется в Системе через сайт Банка. В процессе регистрации Клиент вводит информацию о своих реквизитах, контактном лице, а также вводит номера счетов Клиента, открытых в Банке. Клиент также указывает количество подписей в документе, которое будет необходимо для принятия документа Банком к рассмотрению.
4.5.2.3. В процессе регистрации происходит генерация ключей ЭП Клиента. Ключ ЭП Клиента помещается в специальный файловый криптоконтейнер и на него устанавливается пароль доступа. Ключ ЭП сохраняется на стороне Клиента, а Сертификат регистрируется в Банке.
4.5.2.4. Предварительная регистрация завершается путем распечатки Клиентом 2 (двух) экземпляров Сертификата для каждой ЭП. Каждый Сертификат должен быть заверен подписью лица (Владельца ЭП), на которое оформляется Ключ ЭП, а также подписями уполномоченных лиц и оттиском печати Клиента в соответствии с карточкой с образцами подписей и оттиска печати, принятой Банком.
4.5.2.5. Информация о вновь зарегистрированном Клиенте сохраняется в Системе в течение 30 (тридцати) календарных дней.
4.5.2.6. Для окончательной регистрации Клиента в Системе уполномоченное лицо Клиента представляет 2 (два) экземпляра Сертификата в Банк.
4.5.2.7. В соответствии с Сертификатом сотрудник Банка завершает регистрацию Клиента в ДБО, предоставляя ему право управления своими счетами в Системе.

5. СОГЛАШЕНИЯ СТОРОН ПРИ ИСПОЛЬЗОВАНИИ ЭП

5.1. Стороны соглашаются с нижеследующими условиями применения УНЭП.
5.1.1. используемое в Системе средство криптографической защиты информации «КриптоКОМ» обеспечивает шифрование, контроль Целостности и УНЭП, и предназначено для защиты информации от несанкционированного доступа, подтверждения Подлинности, Целостности и Авторства электронных документов;
5.1.2. использование USB-токена является необходимым средством защиты ключа УНЭП;
5.1.3. для обеспечения дополнительной защиты, в том числе путем формирования списка доверенных получателей платежей Клиента и/или при совершении платежей больше лимита, установленного Клиентом, и/или аутентификации Клиента при входе в Систему могут использоваться:

- MAC-токен;
- SMS-аутентификация.

5.1.3.1. Невозможно использовать одновременно для дополнительной защиты одного и того же действия MAC-токен и SMS-аутентификацию.
5.1.3.2. Использовать MAC-токен и/или SMS-аутентификацию может только Владелец УНЭП.
5.1.4. При использовании УНЭП Клиент обязан использовать ключи ЭП, хранимые в защищенной области памяти USB-токена и являющиеся неизвлекаемыми (неэкспортируемыми).
5.1.5. Стороны признают, что Ключ проверки УНЭП Клиента, указанный в заверенном подписями уполномоченных лиц Клиента и оттиском печати Сертификате ключа проверки ЭП Клиента (Приложение № 8 к Правилам), принадлежит Владельцу ЭП.
5.1.6. При выборе способа входа (Идентификации и аутентификации) в Систему ДБО с использованием ЭП Клиента, записанной на USB-токене, Клиент (в рамках текущей сессии) использует УНЭП, записанную на USB-токене, для подписи всех ЭД, отправляемых в Банк.
Банк.
5.2. Стороны соглашаются с нижеследующими условиями применения ПЭП.
5.2.1. В качестве ПЭП используется электронная подпись, сформированная посредством одноразовых SMS-кодов, направляемых Банком на номера мобильных телефонов Клиента, указан-

ные в Заявлении на подключение к ДБО, и проставленных Клиентом в системе ДБО при подписании ЭД.
5.2.1. Ключом ПЭП являются 2 (два) элемента: номер мобильного телефона Клиента (указанный в Заявлении на подключение к ДБО), идентифицирующий Клиента, и одноразовый SMS-код, проставленный в Системе ДБО при подписании ЭД и подтверждающий факт подписания ЭД данным Клиентом.
5.2.2. ЭД считается подписанным Клиентом при соответствии одноразового SMS-кода, направленного Банком на номер мобильного телефона Клиента, и проставленный им в Системе ДБО при подписании ЭД. В ЭД, воспроизводимом посредством системы ДБО, содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ (данной информацией являются сведения о Клиенте, подписавшем ЭД).
5.2.3. Лица, создающие и (или) использующие ключ ПЭП, обязаны соблюдать его конфиденциальность.
5.2.4. При выборе способа входа (Идентификации и Аутентификации) в Систему ДБО по Логину и Паролю Клиент использует ПЭП в виде Логин/Пароль/SMS для подписи всех ЭД, отправляемых в Банк.
5.3. Стороны признают, что идентификация ЭП Банком является достаточной мерой для установления Подлинности, Целостности и Авторства ЭД. Риск неправомерного использования ЭП Клиента третьими лицами несет Клиент. Клиент заявляет о признании подлинности и надлежащего подписания (включая необходимым количеством лиц) всех документов, заверенных ЭП, пока официально не будет объявлено о Компрометации ключа ЭП.
5.4. Стороны признают, что при произвольном изменении ЭД, заверенного ЭП, Целостность ЭД нарушается, то есть проверка ЭП дает отрицательный результат.
5.5. Стороны признают, что подделка ЭП Клиента, то есть создание подлинной ЭП ЭД от имени Клиента, невозможна без владения ключом ЭП Клиента.
5.6. Стороны признают, что ЭД с ЭП Клиента, создаваемый Системой в Банке, является доказательным материалом для решения спорных вопросов в соответствии с «Процедурой разрешения спорных ситуаций», указанной в разделе 12 Правил. ЭД, не имеющие необходимого количества ЭП, при наличии спорных вопросов, не являются доказательным материалом.
5.7. Стороны признают, что ЭД может исполняться Банком только после того, как под ним собрано столько необходимых ЭП, сколько указано в карточке с образцами подписей и оттиска печати, имеющейся в распоряжении Банка, с учетом распределения по группам (если карточка с образцами подписей и оттиска печати оформлена).
5.8. Стороны признают в качестве единой шкалы времени при работе с Системой московское поясное время. Контрольным является время системных часов аппаратных средств Банка.
5.9. Стороны признают, что ЭД, заверенный ЭП, юридически эквивалентен соответствующему документу на бумажном носителе, оформленному в установленном порядке (имеющему необходимые подписи и оттиск печати), обладает юридической силой и подтверждает наличие правовых отношений между Сторонами. ЭД без необходимого количества ЭП Клиента не имеет юридической силы, Банком не рассматривается и не исполняется.
5.10. Стороны обязуются при обмене ЭД соблюдать требования безопасности электронного документооборота, обеспечивать доступ к аппаратно-программным средствам Системы только уполномоченных лиц, не разглашать третьим лицам способы защиты информации и обеспечения безопасности при работе в Системе, сохранять в тайне ключи ЭП, немедленно информировать другую Сторону обо всех случаях Компрометации ключей ЭП Клиента и ЭП Банка, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств, используемых для электронного документооборота.
5.11 Стороны обязуются использовать специальное ПО - специализированное антивирусное программное обеспечение, используемое для осуществления защиты от ВК, и проводить организованную деятельность по защите своих автоматизированных систем, ПО, средств вычислительной техники, телекоммуникационного оборудования от атак ВК и устранению их последствий.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Банк предоставляет Клиенту необходимые рекомендации для работы с Системой, USB и MAC-токенами, а также производит рассылку сообщений для SMS-аутентификации в целях обеспечения информационной безопасности.
6.2. Банк осуществляет прием ЭД посредством ДБО круглосуточно. ЭД, поступившие до установленного в Банке времени окончания операционного дня, принимаются к обработке в тот же день, документы, поступившие позже указанного времени – на следующий рабочий день.
6.3. При получении ЭД Банк производит проверку подлинности ЭП/ПЭП Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента. В случае отбраковки документ Банком не принимается.
6.3.1. Банк имеет право отказать в исполнении ЭД в случае, если оформление ЭД не соответствует требованиям, установленным законодательством Российской Федерации, нормативными актами Банка России и Банка, а также, если качество ЭД, полученных путем сканирования изображения документов, оформленных первоначально на бумажном носителе, не позволяет Банку прочитать и/или однозначно понять содержащуюся в документе информацию.
6.4. Банк осуществляет в режиме реального времени анализ ЭД на предмет выявления ЭД с признаками несанкционированных операций или с признаками рисковых операций и предпринимать по собственному усмотрению действия, направленные на минимизацию последствий совершения несанкционированных операций или операций повышенного риска.
6.4.1. ЭД с признаками несанкционированных операций – это ЭД, соответствующий одному или нескольким признакам осуществления переводов денежных средств без добровольного согласия Клиента, установленным Банком России и размещенным на его официальном сайте в сети Интернет по адресу: https://cbr.ru/ с учетом требований Федерального закона «О национальной платежной системе» от 27/06/2011 № 161-ФЗ.
6.4.2. ЭД с признаками рисковых операций – это ЭД, соответствующий одному или нескольким признакам мошеннических операций, зафиксированным в аналитической системе Банка, за исключением признаков несанкционированных операций.
6.4.3. При выявлении ЭД с признаками несанкционированных или рисковых операций Банк имеет право приостановить исполнение ЭД на два календарных дня, при этом Клиент информируется о:

- факте приостановлении исполнения ЭД;
- о рекомендациях по снижению риска повторного осуществления Клиентом отказанной или повторной операции;
- о возможности Клиента подтвердить ЭД не позднее одного дня, следующего за днем приостановления ЭД Банком.

6.4.4. Банк имеет право запросить у Клиента дополнительную информацию, подтверждающую, что исполнение ЭД не связано с переводом денежных средств без добровольного согласия Клиента.
6.4.5. Указанное в п. 6.5 информирование осуществляется Банком в следующем порядке (вместе или по отдельности):

- телефонограммой с телефона Банка +7(495) 109-00-14 в рабочее время Банка;
- сообщением в Системе, круглосуточно;
- объявлением при попытке авторизации Клиента в интерфейсе Системы.

6.4.6. При непоступлении от Клиента подтверждения ЭД в срок, который заканчивается в 24 часа дня, следующего за днем приостановления ЭД Банком, ЭД считается непринятым к исполнению. При поступлении от Клиента в указанный срок подтверждения ЭД, Банк исполняет распоряжение Клиента (кроме иных случаев отказа ЭД, указанного в Правилах).
6.4.7. Если, несмотря на направление Клиентом подтверждения ЭД, от Банка России получена информация, относящаяся к Клиенту и/или Системе, и/или иному средству платежа Клиента, о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, Банк приостанавливает исполнение подтвержденного ЭД на два дня со дня направле-

ния Клиентом подтверждения. Банк в порядке, установленном п. 6.4.5 Правил, информирует Клиента о данном факте.

6.4.8. В случаях, указанных в подпунктах п. 6.4 Правил, Клиент подтверждает ЭД:

- уполномоченный представитель Клиента – телефонограммой в рабочее время Банка, если Банк может идентифицировать этого представителя и если ЭД не имеет признаков несанкционированных операций;
- сообщением в Системе круглосуточно, в том числе, в обязательном порядке именно таким образом, если ЭД имеет признаки несанкционированных операций.

6.4.8.1. Если Клиент направляет в Банк подтверждение ЭД в форме сообщения в Системе в нерабочий день Банка, но в пределах, установленного в п. 6.4.6 срока, то такое подтверждение обрабатывается Банком в первый рабочий день, следующий за днем подтверждения.

6.5. Банк обязуется по требованию Клиента блокировать в Системе существующие активные ключи ЭП Клиента и зарегистрировать новые ключи ЭП Клиента в соответствии с представленным в Банк Сертификатом проверки ключа ЭП Клиента. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.

6.6. Банк обязан предоставить Клиенту возможность направления уведомлений об утрате электронного средства платежа и/или использования его без согласия Клиента, в том числе по телефонному звонку Клиента временно блокировать работу Клиента в Системе, если Клиент подтверждает свои полномочия Блокировочным словом. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.

6.7. Банк обязан возобновить работу Клиента в Системе, заблокированную ранее по инициативе Клиента, только при поступлении от Клиента соответствующего заявления (Приложение № 7 к Правилам), заверенного Клиентом оттиском печати и подписями уполномоченных лиц в соответствии с имеющейся в Банке карточкой с образцами подписей и оттиска печати.

6.8. Банк обязан хранить принятые от Клиента ЭД с ЭП/ПЭП в течение сроков, установленных законодательством Российской Федерации.

6.9. При нарушении Клиентом порядка использования Системы в соответствии с Правилами и/или условий договора банковского счета Банк имеет право по своей инициативе приостановить или прекратить использование Клиентом Системы, в том числе ограничить функциональность Системы и не принимать к исполнению ЭД, заверенные ЭП/ПЭП Клиента и требовать предоставления документов, указанных в п. 3.1. Правил, на бумажных носителях в общем порядке.

6.10. Банк приостанавливает использование Клиентом Системы, если от Банка России и/или от федерального органа исполнительной власти в сфере внутренних дел получена информация, относящаяся к Клиенту и/или Системе, и/или иному средству платежа Клиента, о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.

6.10.1. В случае, указанном в п. 6.10 Банк в тот же день уведомляет Клиента о приостановлении использования Системы, а также о праве Клиента подать в порядке, установленном Банком России, в том числе через Банк, заявления об исключении сведений, относящихся к Клиенту, Системе, иному электронному средству платежа Клиента, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента. Указанная информация предоставляется Банком (вместе или по отдельности):

- телефонограммой с телефона Банка +7(495) 109-00-14 в рабочее время Банка;
- сообщением в Системе.

6.11. При наличии подозрений о Компрометации ключей или их неправильном использовании Банк имеет право затребовать от Клиента оформленный в установленном порядке документ на бумажном носителе и не производить исполнение или обработку ЭД.

6.12. В случае, указанном в п. 6.8 Правил, Банк в день блокирования (приостановления или прекращения доступа Клиент к Системе) предоставляет Клиенту информацию о блокировании (приостановлении или прекращении) использования Системы с указанием причины такого блокирования (приостановления или прекращения).

6.13.1. Указанная информация предоставляется Банком:

- телефонограммой по телефону +7(495) 109-00-14 в рабочее время Банка;
- объявлением, при попытке авторизации Клиента в интерфейсе Системы ДБО.

6.14. Банк имеет право на внесение изменений в программное обеспечение Системы, а также требовать от Клиента использовать актуальные версии программного обеспечения.
6.15. Банк имеет право требовать от Клиента использовать USB-токен определенной модели или определенного производителя для генерации и хранения ключей ЭП, использовать MAC-токен и/или SMS-аутентификацию для дополнительной идентификации Клиента, либо использовать иное устройство (технологию), которое Банк примет решение применять для повышения безопасности платежей Клиентов.
6.16. Банк имеет право расторгнуть Договор в порядке, изложенном в разделе 10 Правил, если сочтет, что Клиент пренебрегает мерами информационной безопасности, в частности, не использует в работе устройства (технологии), требуемые Банком для безопасной работы в Системе.
6.17. Банк имеет право на внесение изменений в Правила в одностороннем порядке. Новая редакция Правил вступает в действие через 7 (семь) календарных дней после уведомления Клиента. Уведомление Клиента осуществляется путем рассылки информационного сообщения по Системе, размещения информации на Сайте Банка, а также на информационных стендах в офисах Банка.
6.18. Банк информирует Клиента о совершении каждой операции и/или обработки ЭД с использованием Системы путем направления Клиенту соответствующего уведомления. Обязанность Банка считается выполненной надлежащим образом с момента направления Клиенту уведомления одним или несколькими указанными ниже способами:
6.18.1. Путем изменения статуса ЭД в режиме реального времени. Возможны следующие типы статусов в зависимости от типа ЭД:

- «Новый» - присваивается при создании и сохранении нового ЭД, при редактировании и сохранении существующего ЭД, а также при импорте ЭД. Документ со статусом «Новый» Банк не рассматривает и не обрабатывает;
- «Требует подтверждения» - присваивается платежному поручению после получения необходимого количества подписей, но в случае использования Клиентом MAC-токена или SMS-аутентификации;
- «Подписан» - присваивается в случае, если ЭД подписан, но число подписей под ЭД меньше необходимого;
- «Доставлен» - присваивается в случае, когда число подписей под ЭД соответствует необходимому для рассмотрения документа Банком. Данный статус означает, что ЭД Клиента прошел контроль целостности, формата, ЭП принята Системой, ЭД поставлен в очередь на обработку;
- «На обработке», «На исполнении» - присваивается ЭД при его выгрузке в автоматизированную систему Банка после прохождения всех ее проверок. Данные статусы означают, что ЭД поступил в обработку и находится на исполнении у специалиста Банка;
- «Исполнен» - означает, что ЭД исполнен Банком, то есть финансовый ЭД отражен по Счету (проведен в балансе проводкой), нефинансовый ЭД принят и обработан Банком. Датой принятия ЭД является дата присвоения документу статуса «Исполнен»;
- «Отвергнут» - означает отказ Банка в принятии ЭД. Датой отказа в принятии ЭД является дата присвоения документу статуса «Отвергнут»;
- «Удален» - присваивается ЭД, удаленному пользователем Системы. Удалению подлежат только ЭД в статусе «Новый», «Подписан» или «Отвергнут».

6.18.2. Путем предоставления Клиенту возможности ежедневно и круглосуточно в режиме реального времени получить информацию об остатке денежных средств на Счете, а также о последних операциях по Счету посредством обращения к Системе;
6.18.3. Путем предоставления Клиенту возможности ежедневно и круглосуточно сформировать и распечатать выписку по Счету посредством обращения к Системе;
6.18.4. Путем предоставления Клиенту возможности в период работы Банка получить выписку по Счету на бумажном носителе при его личном обращении в Банк;
6.18.5. Путем предоставления Клиенту возможности получить в режиме реального времени по телефону +7(495) 609-19-19, +7(495) 109-00-14 в рабочее время Банка информацию об остатке

денежных средств на Счете и последних Операциях при условии однозначной идентификации Клиента.
6.19. Уведомления о совершении операции и/или обработке ЭД, ЭД, направленные Банком Клиенту, считаются полученными Клиентом в дату и время присвоения Банком ЭД статуса «Исполнен» или «Доставлен клиенту». Банк не несет ответственности за отсутствие у Клиента доступа к средствам, с использованием которых Клиент может получить уведомление и/или ЭД, либо несвоевременное получение уведомления и/или ЭД, в том числе за сбои в работе интернета, сетей связи, возникшие по независящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом уведомлений и/или ЭД.
6.20. Банк фиксирует направляемые Клиенту уведомления и/или ЭД и хранит их в течение срока, установленного законодательством.
6.21. Банк устанавливает срок действия Сертификата ключа проверки ЭП в соответствии со сроком полномочий Владельцев ЭП и на основании документов, представленных Клиентом, но на срок не более 3 (трех) лет.
6.22. Банк устанавливает и меняет состав Услуг, доступных Клиенту для подключения, получения и отключения самостоятельно и без предварительного уведомления Клиента.

7. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

7.1. На основании имеющихся у Банка лицензий Центра «ЛСЗ» ФСБ России Клиент имеет право осуществлять эксплуатацию предоставленного Банком сертифицированного данным Центром средства криптографической защиты информации в Системе без получения собственной лицензии.
7.2. При конфигурации рабочих мест Клиент обязан учитывать требования, предъявляемые к конфигурации компьютера, на котором устанавливается Система, и его программному обеспечению (Приложение № 3 к Правилам), а также то, что несанкционированное изменение конфигурации может привести к сбою в работе Системы.
7.3. При работе в Системе Клиент обязан использовать USB-токен для генерации и хранения ключей ЭП Клиента и MAC-токен и/или SMS-аутентификацию для дополнительной идентификации Клиента для обеспечения высокого уровня информационной безопасности.
7.3.1. При получении USB и MAC-токена в Банке Клиент обязан подписать Акт приема-передачи (Приложение № 9 к Правилам).
7.4. Клиент обязуется использовать предоставленное СКЗИ только в Системе без права их продажи или передачи каким-либо другим способом иным физическим или юридическим лицам, обеспечивать возможность контроля со стороны федеральных органов за соблюдением требований и условий осуществления лицензионной деятельности.
7.5. Клиент обязан обеспечивать сохранность и целостность программного комплекса Системы, включая предоставленное Банком СКЗИ.
7.6. Клиент обязан незамедлительно (если обнаружение произошло в рабочее время Банка) или не позднее следующего рабочего дня (если обнаружение произошло в нерабочее время Банка) сообщить Банку о возникновении следующих ситуаций:
- несанкционированный доступ или попытка такого доступа к Системе;
- потеря, в том числе кратковременная, контроля над носителями ключа ЭП;
- Компрометация ключей ЭП или логина и пароля для доступа к Системе;
- отказ подтверждения программой проверки ЭП принимаемого электронного документа;
- ошибки при совершении электронных платежей.

7.6.1. Под ошибкой в соответствии с Правилами следует понимать:
- несанкционированный электронный перевод (передача) средств (платежа);
- неверный электронный перевод средств со Счета Клиента;
- ошибку в компьютерных или бумажных расчетах, выполняемых Банком в связи с электронным переводом средств;
- неправильное указание суммы перевода в выписке по Счету;

- подтверждение о принятии Банком электронных платежей, документов и выписок по Счету Клиента, дающих отрицательный результат проверки электронной подписи сотрудника Банка (то есть подпись воспринимается как фальшивая).

7.7. Клиент обязан в случае прекращения использования Системы уничтожить установленное на его компьютерах программное обеспечение Системы, включая СКЗИ.
7.8. Клиент обязан заполнять ЭД в Системе в соответствии с требованиями законодательства и Банка.
7.9. Клиент обязан хранить в секрете и не передавать третьим лицам пароль и носитель с ключом ЭП Клиента, в том числе USB и MAC-токенов, используемый в Системе. Носитель с ключом ЭП должен храниться исключительно у самого лица, для генерации подписи которого он используется. Он не подлежит выносу из служебного помещения Клиента и должен храниться в опечатываемых сейфах. Доступ к рабочему месту, с которого осуществляется доступ к Системе, должен быть ограничен.
7.9.1. Клиент обязан ограничить доступ к устройству (телефону) подвижной радиотелефонной связи, которое зарегистрировано для получения SMS-аутентификации.
7.10. Клиент обязан по требованию Банка прекратить использовать указанный Банком ключ ЭП, сгенерировать новые ключи ЭП и зарегистрировать новый Сертификат проверки ключа ЭП в Банке.
7.11. Клиент обязан обеспечить хранение ЭД, в течение сроков, установленных законодательством Российской Федерации. Документы, подписанные электронной подписью, практическая необходимость в которых отпала, и установленные сроки хранения которых истекли, могут быть уничтожены.
7.12. Для работы с Системой Клиент обязан сформировать ЭП хотя бы для одного лица из числа уполномоченных лиц, указанных им в карточке с образцами подписей и оттиска печати, имеющейся в Банке, а при наличии в Банке подписанного Клиентом Соглашения о праве подписи - хотя бы для одного лица из каждой группы уполномоченных лиц. При этом ЭП каждого из уполномоченных лиц создается на отдельном USB-токене.
7.12.1. Клиент имеет право сформировать дополнительную ЭП на отдельном USB-токене, предназначенную для доступа в Систему для целей просмотра электронных документов и без права их подписания. Такая ЭП может быть сформирована в одном экземпляре для каждого из уполномоченных лиц, указанных в карточке с образцами подписей и оттиска печати, имеющейся в Банке, или для иного лица, полномочия которого подтверждены соответствующей доверенностью.
7.13. Для каждого Владельца ЭП Клиент обязан сформировать с помощью Системы Сертификат ключа проверки ЭП Клиента, который заверяется подписью Владельца ЭП, а также подписями представителей Клиента, указанных в карточке с образцами подписей и оттиска печати, имеющейся в Банке. Сертификат ключа проверки ЭП Клиента также заверяется оттиском печати Клиента (если имеется).
7.13.1. По истечении срока действия Сертификата ключа проверки ЭП Клиента должна быть сгенерирована новая ЭП с формированием нового Сертификата ключа проверки ЭП Клиента.
7.13.2. В случае первичного оформления Сертификата ключа проверки ЭП Клиента, Клиент обязан оформить его на бумажном носителе и заверить собственноручными подписями в порядке, установленном в п. 7.13 Правил.
7.13.3. Новый Сертификат ключа проверки ЭП Клиента может быть оформлен Клиентом в виде ЭД. В этом случае его сканированная копия подписывается действующими ЭП в пределах сроков полномочий Владельцев ЭП и в порядке 7.13 Правил и направляется в Банк средствами Системы. Новый Сертификат ключа проверки ЭП Клиента, оформленный в соответствии с п.7.13 Правил, может быть отправлен в Банк в виде ЭД. В этом случае сканированная копия сертификата подписывается действующими ЭП в пределах сроков полномочий Владельцев ЭП и направляется в Банк средствами Системы.
7.14. Сертификат ключа проверки ЭП вступает в действие в 9-00 рабочего дня, следующего за днем приема Сертификата ключа проверки ЭП Банком, при предоставлении его в Банк в виде ЭД или на бумажном носителе, при этом старый Сертификат ключа проверки ЭП одновременно прекращает свое действие.

7.15. Клиент обязан сгенерировать новый ключ ЭП при изменении лиц, уполномоченных распоряжаться Счетом(-ами), а также при Компрометации ключа ЭП.
7.16. По предложению Банка вносить необходимые изменения в программное и техническое обеспечение для работы Системы.
7.17. Клиент имеет право досрочно прекратить действие своего активного ключа ЭП и потребовать от Банка блокировать этот активный ключ ЭП, оформив уведомление по форме Приложения № 2 к Правилам.
7.18. Клиент имеет право по своему усмотрению генерировать новые ключи ЭП и регистрировать их в Банке.
7.19. Клиент имеет право, позвонив по телефону в Банк, и произнеся Блокировочное слово временно блокировать свою работу в Системе. Такая устная блокировка должна сопровождаться предоставлением письменного уведомления (Приложение № 5 к Правилам) в течение рабочего дня, следующего за днем блокировки.
7.20. Клиент имеет право возобновить свою работу в Системе, которая ранее была заблокирована по инициативе Клиента, представив в Банк Заявление на возобновление предоставления ДБО (Приложение № 7 к Правилам), заверенное оттиском печати, и подписями уполномоченных лиц Клиента, в соответствии с имеющейся в Банке карточкой с образцами подписей и оттиска печати.
7.21. Клиент имеет право представить в Банк Заявление на IP-фильтрацию (Приложение № 10 к Правилам) и воспользоваться соответствующей Услугой Банка.
7.22. Клиент имеет право представить в Банк Заявление на использовании MAC-токена (Приложение № 11 к Правилам) и воспользоваться соответствующей Услугой Банка.
7.23. Клиент обязан применять один из способов получения от Банка уведомлений о совершенных операциях. Обязанности Клиента будут считаться надлежащим образом выполненными, если он не позднее дня совершения операции воспользовался одним из способов доставки уведомлений, указанных в п. 6.15 Правил.
7.24. Клиент обязан внимательно ознакомиться и выполнять требования «Инструкции по обеспечению информационной безопасности в системе ДБО» (Приложение № 12 к Правилам).
7.25. Для целей защиты информации и противодействия осуществлению переводов денежных средств без согласия Клиента, Клиент имеет право устанавливать ограничения (лимиты) максимальной суммы одной операции или суммы операций за период. Данные ограничения устанавливаются Банком в течение трех рабочих дней по:

- Заявлению на дистанционное банковское обслуживание (Приложение № 1), если сведения об ограничениях указаны Клиентом;
- Заявлению на установление ограничений (Приложение № 13).

8. РАЗМЕР И ПОРЯДОК ОПЛАТЫ УСЛУГ БАНКА

8.1. Клиент обязан оплачивать комиссию Банка по предоставлению ДБО, получению USB, MAC-токенов, использованию SMS-аутентификации, а также иных Услуг в соответствии с действующими Тарифами Банка.
8.2. В случае неоплаты или неполной оплаты комиссии Банка в течение 2 (двух) недель, Банк направляет Клиенту уведомление (Приложение № 4 к Правилам) посредством Системы и прекращает предоставлять Клиенту ДБО.
8.3. Присоединяясь к Правилам, Клиент дает Банку заранее данный акцепт на списание без дополнительного согласия комиссии, указанной в п.8.1 Правил, с любого Счета Клиента, открытого в Банке. При этом при необходимости конвертации одной валюты в другую, указанная операция осуществляется за Счет Клиента. Настоящее условие является неотъемлемой частью любого договора Клиента с Банком, который в соответствии с законодательством Российской Федерации может быть квалифицирован как договор банковского счета/ вклада.

9. ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. За неисполнение или ненадлежащее исполнение предусмотренных Договором обязательств Стороны несут ответственность, предусмотренную законодательством Российской Федерации, за исключением возмещения упущенной выгоды.
9.2. При расторжении Договора Стороны несут ответственность по всем электронным документам с активным ключом ЭП, сформированным в Системе, до момента такого расторжения.
9.3. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами ключа ЭП Клиента, а также в случае выявления воздействия вредоносного кода на программно-технические средства Системы Клиента.
9.4. Банк не несет ответственности за сбои в работе линий связи, технических средств и программного обеспечения, повлекшие для Клиента невозможность передачи платежного документа в электронной форме.
9.5. Банк не несет ответственности за исполнение платежных документов Клиента, подготовленных без участия уполномоченных лиц Клиента и переданных в электронной форме, если эти документы имели все необходимые для установления их подлинности реквизиты.
9.6. Клиент несет риск убытков, которые могут возникнуть у него в результате несанкционированного использования его программно-технических средств Системы и его ЭП, в том числе последствий воздействия на эти средства вредоносного кода.
9.7. Клиент несет ответственность за все действия, произведенные с использованием Системы от его имени и с использованием ЭП его уполномоченных лиц.
9.8. Клиент несет ответственности за достоверность информации, направляемой им в Банк в виде ЭД с использованием Системы.
9.9. В случае возникновения у Клиента технических неисправностей или других обстоятельств, препятствующих использованию документов в электронной форме, Клиент может обратиться в Банк с письмом об отмене использования документов в электронном виде на определенный срок или письмом о расторжении Договора (Приложение № 5 к Правилам).
9.10. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих исполнению документов в электронной форме, Банк вправе в одностороннем порядке отменить на неопределенный срок использование документов в электронной форме.
9.11. При отмене использования документов в электронной форме документы, указанные в п. 3.1 Правил, должны представляться Клиентом в Банк на бумажных носителях в общем порядке.
9.12. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы, предоставлять в письменном виде свои оценки, доказательства и выводы.
9.13. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по Договору обязательств в случае возникновения обстоятельств непреодолимой силы, к которым относятся: стихийные бедствия, пожары, аварии, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, актов органов федеральных или местных органов власти и обязательных для исполнения одной из Сторон, прямо или косвенно запрещающих указанные в Правилах виды деятельности или препятствующие выполнению Сторонами своих обязательств, если Сторона, пострадавшая от их влияния, доведет до сведения другой Стороны известие о случившемся в возможно короткий срок после возникновения этих обстоятельств.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Договор вступает в силу с момента акцепта Банком Заявления Клиента, подписанного уполномоченными лицами и заверенного оттиском печати Клиента, в соответствии с имеющейся в Банке карточкой с образцами подписей и оттиска печати. Договор заключается на неопределенный срок.

10.2. Стороны вправе расторгнуть Договор, причем такое расторжение вступает в действие с начала операционного дня рабочего дня, следующего за днем получения Банком уведомления о расторжении Договора, направленного по Системе в виде ЭД или представленного в Банк на бумажном носителе.
10.3. Договор считается автоматически расторгнутым, если в результате расторжения Договоров банковского счета у Клиента не осталось ни одного Счета в Банке.

11. ОБЩИЙ ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

11.1. Споры, возникающие по Договору или в связи с ним, в том числе любой вопрос в отношении его существования, действительности или прекращения, подлежат рассмотрению Сторонами в претензионном порядке. Сторона, заявляющая претензию (требование), обязана направить другой Стороне датированную письменную мотивированную претензию с подробным описанием спорной ситуации. Претензия должна быть передана другой Стороне непосредственно «на руки» или отправлена по почте заказным письмом с описью и уведомлением о вручении. Претензия должна быть рассмотрена Стороной-получателем не позднее 10 (Десяти) рабочих дней.
11.2. В случае возникновении спорных ситуаций между Клиентом и Банком при использовании электронной Системы Стороны обязуются участвовать в рассмотрении споров в соответствии с разделом 12 Правил. При этом обмен электронными документами между Сторонами прекращается.
11.3. Если Стороны не смогут урегулировать возникшие разногласия в претензионном порядке, спор подлежит передаче на рассмотрение в Арбитражный суд г. Москвы.
11.4. Электронные документы, подписанные электронной подписью, допускаются в качестве письменных доказательств. Электронный документ отображается на бумажном носителе путем его распечатки.

12. ПРОЦЕДУРА РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ

12.1. Под спорной ситуацией понимается существование претензий у Клиента к Банку, справедливость которых может быть однозначно установлена по результату проверки Подлинности ЭП Клиента под электронным документом.
12.2. Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ, на основании которого Банк выполнил операции по Счёту Клиента.
12.2.1. Заявление о несогласии с операцией рассматривается Банком в срок, не превышающий 30 (тридцать) календарных дней по операциям, совершенным в Российской Федерации и в срок, не превышающий 60 (шестьдесят) календарных дней по операциям, совершенным за пределами Российской Федерации.
12.3. Банк обязан в течение 5 (пять) рабочих дней от даты подачи заявления Клиента сформировать Экспертную комиссию для рассмотрения заявления. В состав Экспертной комиссии включаются представители Клиента и представители Банка. При необходимости в состав комиссии могут быть включены представители компании-разработчика Системы – ООО «Экспертно-Правовой Центр БИФИТ», а по специальному требованию одной из Сторон – независимые эксперты. Состав Экспертной комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.
12.4. Стороны обязуются способствовать работе Экспертной комиссии и не допускать отказа в предоставлении необходимых документов.
12.5. Стороны обязуются предоставить Экспертной комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в Системе.
12.6. В ходе работы Экспертной комиссии каждая Сторона обязана доказать, что она исполнила обязательства по Договору надлежащим образом.

12.7. Результатом рассмотрения спорной ситуации Экспертной комиссией является определение Стороны, несущей ответственность согласно выводу о Подлинности ЭП Клиента под приложенным документом.
12.8. Экспертная комиссия в течение не более 5 (пять) рабочих дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:
12.8.1. Экспертная комиссия проводит техническую экспертизу Подлинности используемого ключа (ключей) ЭП Клиента.
12.8.1.1. С использованием Системы выполняется распечатка Сертификата ключа проверки ЭП Клиента (Приложение № 8 к Правилам).
12.8.1.2. Результат сверяется с Сертификатом ключа проверки ЭП (Приложение № 8 к Правилам), заверенного подписями уполномоченных лиц и оттиском печати Клиента, в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке. Сверяются идентификатор ключа и его шестнадцатеричный дамп. При обнаружении расхождений ситуация далее не рассматривается как не соответствующая заявленной.
12.8.2. Экспертная комиссия проводит техническую экспертизу электронного документа, заверенного необходимым количеством соответствующих ЭП Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия.
12.8.3. Экспертная комиссия проводит техническую экспертизу подлинности ЭП Клиента в электронном документе.
12.8.3.1. Посредством Системы выбирается документ и выполняется операция «Проверить ЭП».
12.8.3.2. При невозможности получить доступ к документу через Систему, могут использоваться специализированные утилиты от разработчика Системы для выгрузки документа из базы данных и автономной проверки.
12.8.4. На основании данных технической экспертизы Экспертная комиссия составляет акт, содержащий:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- порядок работы членов Экспертной комиссии;
- вывод о подлинности (ложности, приеме, передаче, отзыве и т.п.) оспариваемого электронного документа и его обоснование.

12.8.5. Банк несет ответственность перед Клиентом в случае, когда имело место хотя бы одно из следующих событий:

- Банк не предъявляет электронного документа, переданного Клиентом, на основании которого Банк выполнил операции по Счёту Клиента;
- хотя бы одна ЭП Клиента в оспариваемом электронном документе не признана подлинной;
- Клиент предоставляет Уведомление об отмене действия ключей ЭП Клиента (Приложение № 2 к Правилам), подписанное должностным лицом Банка. При этом указанная в Уведомлении дата окончания действия ключей ЭП Клиента раньше даты, указанной в оспариваемом электронном документе.

12.9. В случае предъявления Банком электронного документа, в котором принадлежность ключей ЭП Клиента, использованных при подписании оспариваемого ЭД, и Подлинность ЭП Клиента признана Экспертной комиссией, Банк перед Клиентом по выполненным со Счёта операциям Клиента ответственности не несёт.
12.10. Если Клиент настаивает на том, что данный документ он не создавал или не подписывал одной или несколькими электронными подписями, Экспертная комиссия может вынести определение о Компрометации ключа (ключей) ЭП Клиента, что не снимает ответственности Клиента за данный документ.
12.11. Если в результате проведенной проверки установлена Подлинность ЭП оспариваемого ЭД, с ключом ЭП, предъявляемым Стороной, получившей оспариваемый ЭД, то Авторство оспариваемого ЭД признается Экспертной комиссией установленным.
12.12. Если в результате проведенной проверки не установлена Подлинность ЭП в оспариваемом ЭД, с ключом ЭП, предъявляемым Стороной, получившей оспариваемый ЭД, то предъявленный для проверки Авторства ЭД признается комиссией ложным.
12.13. Претензии инициатора спора к противоположной Стороне признаются необоснованными, если инициатор спора был обязан в соответствии с установленной разделом 12 Правил проце-

дурой предъявить, но не предъявил Экспертной комиссии полученный им файл, содержащий оспариваемый ЭД, или не предъявил Сертификат ключа проверки электронной подписи противоположной Стороне.

12.14. Отсутствие на клиентском рабочем месте Системы признаков отправки электронного документа, принятого Банком с подлинной ЭП данного Клиента, не является основанием для отказа Клиента от Авторства данного документа.

12.15. По итогам работы Экспертной комиссии составляется итоговый акт, подписываемый всеми членами Экспертной комиссии.

ПРИЛОЖЕНИЕ № 1 ЗАЯВЛЕНИЕ НА ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ДИСТАНЦИОННОЕ БАНКОВСКОЕ ОБСЛУЖИВАНИЕ

Полное наименование корпоративного клиента

Просим АО «МОСКОМБАНК» (далее – Банк) предоставить дистанционное банковское обслуживание (далее – ДБО) ко всем принадлежащим счетам, открытым на основании заключенных между Банком и Клиентом (или которые будут заключены в будущем) договоров банковского счета, вклада, кредитных договоров, договоров факторинга и иных договоров, для которых может быть применимо ДБО.

Для целей аутентификации и подписания электронных документов выбираю следующий вариант работы в ДБО:

☐ - применение простой электронной подписи с SMS-аутентификацией.

Мобильный телефон ; Электронная почта ;

Блокировочное слово .

☐ - применение усиленной электронной подписи. В связи с этим прошу:

☐ - выдать USB-токен в количестве штук; ☐ - выдать MAC-токен в количестве штук.

Просим установить следующие ограничения (лимиты) на операции, совершаемые в ДБО:
руб. - на разовый платеж; руб. - на сумму платежей в день; руб.- на сумму платежей в месяц.

В соответствии со статьей 428 Гражданского кодекса Российской Федерации уведомляем Банк о присоединении к «Правилам дистанционного банковского обслуживания АО «МОСКОМБАНК» для корпоративных клиентов», и подтверждаем, что ознакомлены, понимаем, полностью согласны, принимаем полностью без каких-либо оговорок и изъятий, а также уведомлены о наличии рисков и возможности несанкционированного доступа к банковским счетам при несоблюдении требований по обеспечению безопасности и обязуемся исполнять указанные Правила и Тарифы Банка.

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

						2	**0**		

Отметки АО «МОСКОМБАНК»

В соответствии с «Правилами дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов», а также их акцептом настоящим Заявлением, а вместе образующих Договор, подключить Клиента к дистанционному банковскому обслуживанию.

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

М.П.

ПРИЛОЖЕНИЕ № 2 УВЕДОМЛЕНИЕ ОБ ОТМЕНЕ ДЕЙСТВИЯ КЛЮЧЕЙ ЭП

МОСКОМБАНК
Commercial Bank of Moscow

УВЕДОМЛЕНИЕ ОБ ОТМЕНЕ ДЕЙСТВИЯ КЛЮЧЕЙ ЭП

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов» уведомляем АО «МОСКОМБАНК» о том, что с считается недействительным ключ ЭП со следующим идентификатором:

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

						2	**0**		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ

Для работы с Системой необходимо:

1. Компьютер с USB портом.

2. Одна из операционных систем:
   - Windows 7 и более поздние версии;
   - Linux 32-bit/64-bit;
   - Mac OS X.

3. Дополнительное оборудование:
   - Принтер.

4. Программное обеспечение:
   - Один из Web-браузеров:
     - Internet Explorer 10+;
     - Firefox;
     - Opera;
     - Chrome;
     - Safari;
   - Плагин к браузеру «Bifit signer».

ПРИЛОЖЕНИЕ № 4 УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

МОСКОМБАНК
Commercial Bank of Moscow

УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания АО «МОСКОМБАНК» для корпоративных клиентов», уведомляем Вас о том, что с « » 20 г. дистанционное обслуживание будет приостановлено в связи с неоплатой или неполной оплатой данной услуги Банка.

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 5 ЗАЯВЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания АО «МОСКОМБАНК» для корпоративных клиентов» просим Вас прекратить предоставление данной услуги на указанном ниже условии:

☐ - на период до ;

☐ - считать Договор о дистанционном банковском обслуживании расторгнутым.

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

						2	**0**		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 6 ЗАЯВЛЕНИЕ НА ОТКЛЮЧЕНИЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ НЕКОТОРЫХ СЧЕТОВ

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ОТКЛЮЧЕНИЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ НЕКОТОРЫХ СЧЕТОВ

Полное наименование корпоративного клиента

Просим АО «МОСКОМБАНК» (далее – Банк) отключить дистанционное банковское обслуживание указанных ниже счетов:

Номер счета	
Номер счета	
Номер счета	

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

«__» **20**__ г.

Отметки АО «МОСКОМБАНК»

В соответствии с «Правилами дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов» отключить дистанционное банковское обслуживание указанных выше счетов Клиента.

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

«__» 20__ г.

М.П.

ПРИЛОЖЕНИЕ № 7
ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ПРЕДОСТАВЛЕНИЯ ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ПРЕДОСТАВЛЕНИЯ ДБО

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов» просим Вас снять блокировку с нашей работы в Системе и возобновить предоставление ДБО.

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

						2	**0**		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 8
СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА

МОСКОМБАНК
Commercial Bank of Moscow

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА

1. Наименование организации: _____
_____
2. Адрес места _____
нахождения: _____
3. ОГРН Клиента: _____ ИНН Клиента: _____
4. Сведения о владельце ключа
Фамилия, Имя, Отчество:_____
Должность: _____
5. Паспорт: _____ серия _____
номер _____ дата выдачи «_____» _____ года
кем выдан _____
6. Идентификатор ключа: _____
7. Наименование криптосредств: _____
8. Алгоритм: _____ ID набора параметров алгоритма: _____
9. Дата начала действия: «_____»_____20___г.
10. Дата окончания действия: «_____»_____20___г.
11. Представление ключа проверки электронной подписи в шестнадцатеричном виде:

```
50  E3  CA  1C  C5  2E  97  ED  83  43  FE  F9  FA  2E  27  EF
6F  4D  F1  20  ID  B8  5B  F5  3C  57  C1  3D  3F  99  41  73
7A  F6  91  E7  07  9B  0A  B8  AD  83  F7  9E  FE  2A  3B  30
0D  F0  76  C4  39  92  83  6E  78  5B  D1  10  55  23  E6  E8
```

Владелец ключа электронной подписи _____
фамилия, инициалы подпись

Уполномоченные лица Клиента

_____ **М.П.**
должность фамилия, инициалы подпись

_____
должность фамилия, инициалы подпись

						2	0		

Отметки АО «МОСКОМБАНК»
Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

ПРИЛОЖЕНИЕ № 9
АКТ ПРИЕМА-ПЕРЕДАЧИ

МОСКОМБАНК
Commercial Bank of Moscow

АКТ ПРИЕМА-ПЕРЕДАЧИ

Полное наименование корпоративного клиента

_____

_____

На основании «Правил дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов» получено:

☐ - USB-токен, в количестве шт. USB-токен – аппаратное USB-устройство, в котором реализованы российские криптоалгоритмы и имеется защищенная область памяти. Устройство позволяет генерировать и безопасно хранить ключи ЭП в неизвлекаемом виде;
☐ - MAC-токен, в количестве шт. MAC-токен - аппаратное устройство, позволяющие генерировать цифровой код для подтверждения платежного документа исходя из его реквизитов, а также для дополнительной идентификации Клиента, подтверждения платежей больше установленного лимита и создания списка доверенных получателей платежей Клиента.

№ п/п	Идентификатор USB/MAC-токена
1	
2	
3	
4	
5	

Уполномочиваем Банк списать комиссию за выдачу токена, в соответствии с Тарифами Банка:

☐ - с нашего текущего счета у Вас № ;

☐ - принять наличными в кассу Банка.

От Клиента _____ _____
подпись фамилия, инициалы

От Банка _____ _____
подпись фамилия, инициалы

М.П.

						2	**0**		

ПРИЛОЖЕНИЕ № 10
ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания АО «МОСКОМБАНК» для корпоративных клиентов» просим Вас:

☐ - отменить ранее установленные ограничения;

☐ - установить возможность доступа в Системе со следующих IP адресов (хосты или подсети):

№ п/п	IP адрес/маска
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

20

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы | подпись

20

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 11
ЗАЯВЛЕНИЕ НА ИСПОЛЬЗОВАНИЕ MAC-ТОКЕНА И/ИЛИ SMS-АУТЕНТИФИКАЦИИ

ЗАЯВЛЕНИЕ НА ИСПОЛЬЗОВАНИЕ MAC-ТОКЕНА

Полное наименование корпоративного клиента

На основании «Правил дистанционного банковского обслуживания в АО «МОСКОМБАНК» для корпоративных клиентов» просим Вас, для следующих MAC-токенов и/или устройств (телефонов) подвижной радиотелефонной связи:

№ п/п	Идентификатор токена	Номер телефона	ФИО Владельца ЭП
1			
2			
3			
4			

☐ - установить дополнительную идентификацию одноразовым цифровым кодом при подключении к Системе с помощью MAC-токена;

☐ - отменить ранее установленную дополнительную идентификацию одноразовым цифровым кодом при подключении к Системе с помощью MAC-токена;

☐ - установить дополнительное подтверждение одноразовым цифровым кодом при совершении платежей свыше руб. с помощью MAC-токена;

☐ - отменить ранее установленное дополнительное подтверждение одноразовым цифровым кодом при совершении платежей с помощью MAC-токена;

☐ - установить возможность создания списка доверенных получателей платежей с помощью MAC-токена;

☐ - отменить возможность создания списка доверенных получателей платежей с помощью ☐ - MAC-токена.

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

☐☐☐☐☐☐**2 0**☐☐

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

☐☐☐☐☐☐2 0☐☐

ПРИЛОЖЕНИЕ № 12
РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

МОСКОМБАНК
Commercial Bank of Moscow

РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА

В области информационной безопасности АО «МОСКОМБАНК» рекомендует Клиенту:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Системы. Признаком установки защищённого соединения является наличие информации о протоколе https в адресной строке используемого клиентом браузера, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.

2. Осуществлять вход в Систему только через Сайт Банка *москомбанк.рф (https://www.moscombank.ru)*.

3. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену *москомбанк.рф (https://www.moscombank.ru)*, сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефонам: (495) 109-00-14. Банк не осуществляет рассылку электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Системы.

4. Извлекать из компьютера USB-токен или другой носитель, содержащий ключ электронной подписи, сразу после завершения работы с ним в Системе.

5. Обеспечить использование USB/MAC-токенов только ответственным сотрудником, уполномоченным на то соответствующим распорядительным документом.

6. Не передавать токены или другие носители, содержащие ключ электронной подписи неуполномоченным сотрудникам Клиента (в том числе ИТ-сотрудникам, а также сотрудникам Банка) для проверки работы Системы, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить USB-токен или другой носитель ЭП к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентской части Системы, и лично ввести пароль, сохраняя его конфиденциальность.

7. Хранить токены или другие носители, содержащие ключи электронной подписи, в надежном месте, исключающем доступ к нему неуполномоченных лиц и повреждение материального носителя. Вся ответственность за сохранность и использование ключей ЭП полностью лежит на Клиенте, как единственном их владельце

8. Не отлучаться от устройства с установленным ДБО в период активной сессии с Системой, либо завершить активную сессию ДБО.

9. Использовать виртуальную клавиатуру. Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками. Виртуальная клавиатура появляется при входе в Систему. При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе (если пароль содержит заглавную букву или символ, нажмите клавишу Shift, переключение между русским и английским алфавитом - клавиша Рус/Lat, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите Enter.

10. Для получения сообщений для SMS-аутентификации ограничить доступ к устройству (телефону) подвижной радиотелефонной связи, которое зарегистрировано для этих целей.

11. Обеспечить отсутствие доступа третьих лиц к устройству и сим-карте, посредством которых осуществляется доступ к номеру телефона, используемого при работе в системе ДБО (в том числе для формирования простой электронной подписи), в том числе с использованием штатных средств ограничения доступа (PIN-код, графический ключ, Touch ID, Face ID и т.п).

12. Обеспечить сокрытие отображения текстов смс-сообщений или PUSH-уведомлений на заблокированном мобильном устройстве.

13. Не подключаться к общедоступным Wi-Fi сетям.

14. Не записывать используемый Пароль там, где доступ к нему могут получить посторонние лица.

15. Незамедлительно произвести блокировку сим-карты в случае утери или кражи мобильного устройства или сим-карты.

16. Написать заявление сотовому оператору о запрете принимать обращения на блокировку/разблокировку/замену сим-карты от третьих лиц по доверенности.

17. В случае обнаружения блокировки Вашей сим-карты без Вашего ведома немедленно заблокировать доступ в Системе, обратившись в службу поддержки по телефону на сайте Банка.

18. При подписании платежного документа в системе ДБО осуществлять сверку реквизитов, полученных в SMS-сообщении, с кодом подтверждения, с реквизитами документа, отображаемыми в интерфейсе Системы.

19. При использовании услуг SMS-информирования об операциях проверять реквизиты в направляемых Банком информационных сообщениях о проведенных операциях. В случае возникновения подозрений о мошеннических действиях незамедлительно сообщать Банку по официальному номеру телефона, указанному на сайте Банка.

20. В случае выявления явных или косвенных признаков Компрометации ключей ЭП или вредоносных программ в компьютере, используемом для работы в Системе, незамедлительно уведомить об этом Банк по телефонам: (495) 109-00-14, либо лично явившись в Банк с целью блокирования скомпрометированных ключей ЭП с последующей их заменой. К событиям, связанным с Компрометацией ключей ЭП относятся, включая, но не ограничиваясь, следующие:

- утеря USB-токена или другого устройства, содержащего ключ электронной подписи, в том числе с последующим обнаружением;
- выход USB-токена или другого устройства, содержащего ключ электронной подписи, когда невозможно достоверно определить причину этого события (доказательно не

опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

- обнаружение факта или угрозы использования (копирования) ключа ЭП и/или доступа к Системе с использованием ключа ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Системы, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение вредоносных программ в компьютере, используемом для работы в Системе;
- увольнение ответственного сотрудника Клиента, имевшего доступ к ключу ЭП.

21. Обеспечивать конфиденциальность использования пароля Клиента для доступа к ключу ЭП. Пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.

22. Применять на рабочем месте лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, спам-фильтры.

23. Производить периодическую (не реже 1 раза в 3 месяца) смену пароля ключей ЭП, а так же в случае Компрометации ключа или по требованию Банка. Пароли должны выбираться исходя из следующих требований:

- длина пароля не менее 8 символов;
- пароль должен состоять из больших и маленьких букв, цифр и специальных символов (+ = * и т.д.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения и т.д.), а также общепринятые сокращения (qwerty, qwerty123, 12345678 и т.д.);
- при смене пароля он должен отличаться от предыдущего не менее чем в 2х позициях.

24. Самостоятельно настроить используемое оборудование и программное обеспечение для работы с сетью Интернет по защищенному протоколу https.

25. Не использовать на рабочем месте любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer, AnyDesk, Ammy Admin и др.). Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

26. При использовании мобильного устройства установить на него антивирусное программное обеспечение и пароль доступа к устройству, не использовать мобильное устройство с расширенными правами (Jailbreak/Root), так как это значительно снижает уровень обеспечения безопасности устройства. Регулярно устанавливать обновления для Вашего устройства и установленного антивирусного программного обеспечения, защитить свое мобильное устройство кодом блокировки экрана, паролем или отпечатком пальца.

27. Не устанавливать на мобильное устройство, используемое для приема SMS-сообщений с подтверждающим одноразовым Паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим Клиентам ссылки или указания на установку приложений.

28. При утрате мобильного устройства или SIM-карты, используемых для приема SMS-сообщений с подтверждающим одноразовым Паролем, немедленно обратиться к своему оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Системе и проверки последних платежей.

29. Выделить для использования в Системе отдельный компьютер, настроенный на работу только с сервером Банка, а при наличии двух ключей электронной подписи – двух выделенных компьютеров, так как вероятность вирусного заражения обоих компьютеров резко снижается.

30. Исключить доступ к компьютерам, используемым для работы в Системе, посторонним лицам и персоналу организации Клиента, не уполномоченному на работу в Системе и/или обслуживание компьютеров.

31. На компьютерах, используемых для работы в Системе, исключить посещение всех интернет-сайтов, кроме используемых для входа в Систему, а также исключить установку развлекательных и игровых программ.

32. Использовать только лицензионное ПО (операционные системы, офисные пакеты и пр.), обеспечить автоматическое обновление системного и прикладного ПО, исключить использование самодельных «сборок» и взломанного программного обеспечения.

33. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями. Обеспечить использование ключей электронной подписи и MAC-токенов только ответственными сотрудниками, не оставлять USB-токен подключенным к компьютеру постоянно, использовать USB-токен только для подписания документов в Системе.

34. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Системе только с указанных Клиентом IP адресов/сетей).

В области социальной инженерии АО «МОСКОМБАНК» рекомендует Клиенту:

1. Обращать внимание на следующие признаки мошенничества:
   - мошенник обращается с неизвестного номера телефона;
   - мошенник представляется сотрудником Банка, Центрального Банка, Федеральных органов исполнительной власти (полиция, следователи, сотрудники Федеральной службы безопасности), операторов связи;
   - Клиенту предлагается или какая-то выгода или описывается проблема и предлагается путь решения;
   - от Клиента требуют сообщить номера карты, ПИН-код, логин и пароль от банковских приложений, подтвердить код по СМС, перейти по ссылке в СМС или e-mail сообщении, т.е. провести компрометацию конфиденциальных данных;
   - от Клиента требуют провести мгновенную оплату, перевод денежных средств;
   - от Клиента требуют быстрого принятия решения, немедленной реакции;
   - возражают против того, чтобы Клиент позвонил позже, препятствуют разъединению телефонного звонка.

ПРИЛОЖЕНИЕ № 13
ЗАЯВЛЕНИЕ НА УСТАНОВЛЕНИЕ ОГРАНИЧЕНИЙ (ЛИМИТОВ)

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА УСТАНОВЛЕНИЕ ОГРАНИЧЕНИЙ (ЛИМИТОВ)

Полное наименование корпоративного клиента

Просим установить следующие ограничения (лимиты) на операции, совершаемые в ДБО:

- руб. - на разовый платеж;
- руб. - на сумму платежей в день;
- руб. - на сумму платежей в месяц.

Уполномоченные лица:

должность	фамилия, инициалы	подпись
должность	фамилия, инициалы	подпись

М.П.

						2	**0**		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		