УТВЕРЖДЕНЫ
Правлением ПАО «МОСКОМБАНК»
Протокол №01-05/29 от 29.10.2015 г.
Введено в действие 05.11.2015 г.
Приказом № 01-08/117 от 29.10.2015 г.

МОСКОМБАНК
Commercial Bank of Moscow

ПРАВИЛА
дистанционного обслуживания банковских счетов
ПАО «МОСКОМБАНК»
для корпоративных клиентов
(версия 3.5)

Москва
2015

1. Определения

Банк – ПАО «МОСКОМБАНК»;

Клиент – корпоративный клиент Банка – юридическое лицо или индивидуальный предприниматель;

Сторона, Стороны – Банк и/или Клиент;

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

Система «iBank 2» - электронное средство платежа, позволяющее Клиенту составлять, удостоверять и передавать в Банк распоряжения в целях осуществления перевода денежных средств с использованием информационно-телекоммуникационных технологий, технически представляющее из себя совокупность программно-аппаратных средств и используемых на стороне Клиента и Банка;

ДОБС (Дистанционное Обслуживание Банковских Счетов) – технологии и процедуры, проводимые Клиентом и Банком с целью дистанционного обслуживание банковских счетов в системе «iBank 2»;

Правила – настоящие «Правила дистанционного обслуживания банковских счетов ПАО «МОСКОМБАНК» для корпоративных клиентов»;

Заявление – Заявление на дистанционное обслуживание банковских счетов, направляемое Клиентом Банку;

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

Электронный документ (ЭД) – совокупность информации с цифровой форме, содержащая финансовый документ, информационное или служебное сообщение в системе;

Э**лектронная 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 является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Усиленной неквалифицированной электронной подписью 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 «iBank 2», 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 «iBank 2», и предназначенный для проверки Банком подлинности ЭП электронного документа, сформированного Клиентом;

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

Сертификат ключа проверки ЭП Клиента – бумажный документ, с представленным в шестнадцатеричном виде ключом проверки ЭП Клиента, датой начала и окончания действия ключа ЭП Клиента, заверенный подписями уполномоченных лиц Клиента и оттиском печати Клиента в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке;

Активный ключ ЭП Клиента – ключ ЭП Клиента, зарегистрированный Банком в системе «iBank 2», и используемый Клиентом для работы в системе «iBank 2»;

Средство криптографической защиты информации (СКЗИ) – СКЗИ Крипто-КОМ 3.3 компании ЗАО «Сигнал-КОМ», входящее в состав системы «iBank 2» и имеющее сертификаты ФСБ России СФ/124-2061, СФ/124-2062 от 01.02.2013 г., 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 – это компактное устройство, оснащенное дисплеем и цифровой клавиатурой, предназначенное для вычисления цифрового кода 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 «iBank 2»;

IP-фильтрация - фильтрация IP адресов, позволяющая осуществлять вход в систему «iBank 2» только с определенных компьютеров. Используется для повышения информационной безопасности при работе в системе ДОБС 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 «iBank 2». Блокировочное слово может быть использовано Клиентом (например, в случае компрометации ключа) для блокирования своей работы в «iBank 2» 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 «iBank 2» 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 «iBank 2»;

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 «iBank2», 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.

2. Общие положения

2.1. Настоящие Правила определяют порядок предоставления ПАО «МОСКОМБАНК» ДОБС, позволяющий получать дистанционный доступ к банковским счетам, передавать электронные расчетные документы, принимать выписки по банковским счетам, а также передавать и принимать информационные и сервисные сообщения.
2.2. Договор, образованный настоящими Правилами и Заявлением (Приложение № 1 к настоящим Правилам), является неотъемлемой частью всех договоров банковского счёта, заключённых между Банком и Клиентом, а также договоров банковского счёта, которые могут быть заключены Сторонами в будущем.
2.2.1. По заявлению Клиента (Приложение № 13 к настоящим Правилам) некоторые договоры банковского счета, заключенные между Банком и Клиентом могут быть исключены из общего правила, указанного в п. 2.2.
2.3. Клиент подтверждает, что до присоединения к настоящим Правилам ознакомился и проинформирован об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа.

3. Документы

3.1. Стороны договорились использовать в электронной форме документы, предусмотренные законодательством РФ, нормативными актами Банка России и Банка, регулирующими осуществление безналичных расчетов в РФ (платежные поручения, заявления на перевод иностранной валюты, поручения на покупку/продажу иностранной валюты, ведомости к платежным документам, выписки по счетам, запросы, письма, уточнения, отзывы, уведомления и иные документы, не являющиеся платежными, составленные в свободном формате, в том числе документы валютного контроля и т.п.).
3.2. По требованию Банка Клиент обязан в двухдневный срок предоставить на бумажном носителе экземпляр любого документа, указанного в п.3.1. настоящих Правил, подписанного уполномоченными лицами и заверенного оттиском печати Клиента, в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке.
3.3. Документы, указанные в п.3.1. настоящих Правил, изготавливаются в электронной форме на основе использования предоставляемого Банком программного обеспечения системы «iBank 2». Форматы платежных документов в электронной форме формируются системой «iBank 2».
3.4. Перечень реквизитов платежных документов в электронной форме должен соответствовать реквизитам соответствующего расчетного документа, форма (формат) которого установлена законодательством РФ и правилами Банка.
3.5. Отображение электронного платежного документа на бумажном носителе осуществляется в виде, указанном в п.3.4. настоящих Правил путём его распечатки на принтере исключительно через систему «iBank 2».
3.6. Подлинником электронного документа является электронный образ документа в оговоренном формате, который содержит текст документа и ЭП уполномоченных(-ого) лиц(а) Стороны, подписавших этот документ, с положительным результатом проверки подлинности ЭП, произведенной программными средствами системы «iBank 2», с использованием ключей проверки ЭП, зарегистрированных в установленном настоящими Правилами порядке. Результаты проверки подлинности фиксируются с использованием средств системы «iBank 2».

4. Соглашения Сторон

4.1. Стороны признают, что:
4.1.1. используемое в системе «iBank 2» средство криптографической защиты информации «Крипто-КОМ 3.3», которое обеспечивает шифрование, контроль Целостности и ЭП, и предназначено для защиты информации от несанкционированного доступа, подтверждения Подлинности, Целостности и Авторства электронных документов;
4.1.2. использование USB токена в системе «iBank 2» является необходимым средством защиты ключа ЭП;
4.1.3. использование MAC токена является дополнительной мерой защиты электронных платежей при использовании системы «iBank 2»;

4.1.4. использование IP-фильтрации и MAC токена в системе «iBank 2» являются необходимыми дополнительными мерами защиты при идентификации Клиента, как вместе, так и по отдельности;

4.1.5. использование MAC токена в системе «iBank 2» является необходимой дополнительной мерой защиты при совершении платежей больше лимита установленного Клиентом.

4.1.6. использование MAC токена является дополнительной мерой защиты, обеспечивающей формирование списка доверенных получателей платежей Клиента.

4.2. В соответствии с положениями Федерального Закона РФ от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» используемая в системе «iBank 2» электронная подпись на основе российских криптоалгоритмов признается сторонами **усиленной неквалифицированной** ЭП. В соответствии с рекомендациями Банка Клиент обязан использовать ключи ЭП, хранимые в защищенной области памяти USB токена и являющиеся неизвлекаемыми (неэкспортируемыми).

4.3. Стороны признают, что идентификация ЭП Банком является достаточной мерой для установления Подлинности, Целостности и Авторства электронных документов. 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.

4.4. Стороны признают, что при произвольном изменении электронного документа, заверенного ЭП, целостность ЭД нарушается, то есть проверка ЭП дает отрицательный результат.

4.5. Стороны признают, что подделка ЭП Клиента, то есть создание подлинной ЭП электронного документа от имени Клиента, невозможна без владения ключом ЭП Клиента.

4.6. Стороны признают, что электронные документы, заверенные (необходимым количеством) ЭП, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке (имеющим необходимые подписи и оттиск печати), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. Электронные документы без необходимого количества ЭП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

4.7. Стороны признают, что электронные документы с ЭП Клиента, создаваемые системой «iBank 2» в Банке, являются доказательным материалом для решения спорных вопросов в соответствии с «Порядком разрешения спорных ситуаций» раздела 11 настоящих Правил. Электронные документы, не имеющие необходимого количества ЭП, при наличии спорных вопросов, не являются доказательным материалом.

4.8. Стороны признают, что ключ проверки ЭП Клиента, указанный в заверенном подписями уполномоченных лиц Клиента и оттиском печати Сертификате ключа проверки ЭП Клиента (Приложение № 8 к настоящим Правилам), принадлежит Клиенту.

4.9. Стороны признают, что электронный документ 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.

4.10. Стороны признают в качестве единой шкалы времени при работе с системой «iBank 2» Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.

4.11. Стороны обязуются при обмене электронными документами соблюдать требования безопасности электронного документооборота, обеспечивать доступ к аппаратно-программным средствам системы «iBank2» только уполномоченных лиц, не разглашать третьим лицам способы защиты информации и обеспечения безопасности при работе в системе «iBank2», 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.

4.12. 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.

5. Права и обязанности Банка

5.1. Банк предоставляет Клиенту необходимые рекомендации для работы с системой «iBank 2», USB и MAC токены для обеспечения информационной безопасности, а также оказывает услуги по установке необходимого программного обеспечения на компьютеры Клиента.
5.2. Банк осуществляет прием электронных документов посредством ДОБС круглосуточно. Электронные документы, поступившие до установленного в Банке времени окончания операционного дня, принимаются к исполнению в тот же день, документы, поступившие позже указанного времени – на следующий рабочий день.
5.3. При получении электронного документа Банк производит проверку подлинности ЭП Клиента, проверку правильности заполнения реквизитов документа, проверку на возможность возникновения дебетового сальдо на расчётном счёте Клиента. В случае отбраковки документ Банком не принимается.
5.4. Банк обязуется по требованию Клиента блокировать в системе «iBank 2» существующие активные ключи ЭП Клиента и зарегистрировать новые ключи ЭП Клиента в соответствии с представленным в Банк Сертификатом. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.
5.5. 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 «iBank 2», если Клиент подтверждает свои полномочия Блокировочным словом. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.
5.6. Банк обязан возобновить работу Клиента в системе «iBank 2», заблокированную ранее по инициативе Клиента, только при поступлении от Клиента соответствующего заявления (Приложение № 7 к настоящим Правилам), заверенного Клиентом оттиском печати и подписями уполномоченных лиц в соответствии с имеющейся в Банке карточке с образцами подписей и оттиска печати.
5.7. Банк обязан хранить принятые от Клиента данные с электронной подписью в течение пяти лет.
5.8. Банк имеет право по своему усмотрению, без уведомления Клиента и без объяснения причин, блокировать активный ключ(и) ЭП Клиента и потребовать от Клиента смены ключа(ей) ЭП.
5.9. Банк имеет право по своему усмотрению, без уведомления Клиента и без объяснения причин, блокировать доступ Клиента к ДОБС, не принимать к исполнению электронные документы, заверенные ЭП Клиента, при этом расчетные документы, указанных в п.3.1. настоящих Правил, должны представляться Клиентом в Банк на бумажных носителях в общем порядке.
5.10. При наличии подозрений о компрометации ключей или их неправильном использовании Банк имеет право затребовать от Клиента оформленного в установленном порядке документа на бумажном носителе и не производить исполнения электронного документа, сообщив об этом клиенту не позднее следующего банковского дня со дня получения соответствующего электронного документа.
5.11. Банк имеет право на внесение изменений в программное обеспечение системы «iBank 2».
5.12. Банк имеет право требовать от Клиента использовать USB токен определенной модели или определенного производителя для генерации и хранения ключей ЭП, использовать MAC токен для дополнительной идентификации Клиента, либо использовать иное устройство, которое Банк примет решение применять для повышения безопасности платежей Клиентов.
5.13. Банк имеет право по собственному усмотрению расторгнуть Договор в порядке, изложенном в разделе 9 настоящих Правил, если сочтет, что Клиент не предпринимает достаточных мер по информационной безопасности электронных платежей, в частности, не использует в работе USB/MAC токены, либо иные устройства, требуемые Банком.
5.14. Банк имеет право на внесение изменений в настоящие Правила в одностороннем порядке. Новая редакция Правил вступает в действие через 15 календарных дней после уведомления Клиента. Уведомление Клиента осуществляется путем рассылки информационного сообщения по системе «iBank 2», размещения информации на сайте Банка *москомбанк.рф* (https://www.moscombank.ru), а также на информационных стендах в офисах Банка.

5.15. Банк информирует Клиента о совершении каждой операции с использованием системы «iBank2» путем направления Клиенту соответствующего уведомления. Обязанность Банка считается выполненной надлежащим образом с момента направления Клиенту уведомления одним или несколькими указанными ниже способами:

5.15.1. Путем изменения статуса его распоряжения на перевод денежных средств в режиме реального времени. Возможны четыре вида статуса:

- «Принято» - означает, что распоряжение Клиента прошло контроль целостности, формата и ЭП электронного документа принято системой iBank 2» в очередь на обработку;
- «На обработке» - означает, что распоряжение поступило в обработку и будет рассмотрено специалистом Банка в ближайшее время;
- «На исполнении» - означает, что распоряжение направлено получателю платежа (в Банк получателя платежа),
- «Исполнено» - означает, что распоряжение Клиента доставлено получателю платежа (в Банк получателя платежа);

5.15.2. 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 «iBank2»;

5.15.3. Путем предоставления Клиенту возможности ежедневно и круглосуточно сформировать и распечатать выписку по Счету посредством обращения к системе «iBank2»;

5.15.4. Путем предоставления Клиенту возможности в период работы Банка получить выписку по Счету на бумажном носителе при его личном обращении в Банк;

5.15.5. Путем предоставления Клиенту возможности получить в режиме реального времени по телефону +7(495) 609-19-19 в рабочее время Банка информацию об остатке денежных средств на Счете и последних Операциях при условии однозначной идентификации Клиента.

5.16. Уведомление о совершении операции считается полученным Клиентом по истечении трех часов с момента его направления Банком. Банк не несет ответственности за отсутствие у Клиента доступа к средствам, с использованием которых Клиент может получить уведомление, либо несвоевременное получение уведомления, 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 о совершении операции.

5.17. Банк фиксирует направляемые Клиенту уведомления и хранит их в течение трех лет.

6. Права и обязанности Клиента

6.1. Клиент имеет право, представив в Банк Заявление на установку программного обеспечения (Приложение № 6 к настоящим Правилам), воспользоваться соответствующей услугой Банка, в том числе с выездом специалиста Банка на территорию Клиента.

6.2. 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 «iBank 2» без получения собственной лицензии.

6.3. При конфигурации рабочих мест Клиент обязан учитывать требования, предъявляемые к конфигурации компьютера, на котором устанавливается система «iBank 2», и его программному обеспечению (Приложение № 3 к настоящим Правилам), а также то, что несанкционированное изменение конфигурации может привести к сбою в работе системы «iBank 2».

6.4. Перед началом эксплуатации системы «iBank 2» Клиент обязан получить в Банке (скачать с сайта Банка москомбанк.рф (https://www.moscombank.ru) и самостоятельно установить на своем рабочем месте СКЗИ и драйвер USB токена (с учетом п.6.1. настоящих Правил).

6.4.1. При работе в системе «iBank 2» Клиент обязан использовать USB токен для генерации и хранения ключей ЭП Клиента и MAC токен для дополнительной идентификации Клиента для обеспечения высокого уровня информационной безопасности.

6.4.2. При получении USB и MAC токена в Банке Клиент обязан подписать Акт приема-передачи (Приложение № 9 к настоящим Правилам).

6.5. Клиент обязуется использовать предоставленное СКЗИ только в системе «iBank 2», 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.

6.6. Клиент обязан обеспечивать сохранность и целостность программного комплекса системы «iBank 2», включая предоставленное Банком СКЗИ.

6.7. Клиент обязан незамедлительно сообщить Банку, но не позднее следующего рабочего дня с момента обнаружения, о возникновении следующих ситуаций:

- несанкционированный доступ или попытка такого доступа к системе «iBank 2»;
- потеря, в том числе кратковременная, контроля над носителями ключа ЭП;
- компрометация ключей ЭП или логина и пароля для доступа к системе «iBank 2»;
- отказ подтверждения программой проверки ЭП принимаемого электронного документа;
- ошибки при совершении электронных платежей.

6.7.1. Под ошибкой в целях настоящих Правил 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 (т.е. подпись воспринимается как фальшивая).

6.8. Клиент обязан в случае прекращения использования системы «iBank 2» уничтожить установленное на его компьютерах программное обеспечение системы «iBank 2», включая СКЗИ.

6.9. Клиент обязан заполнять электронные документы в системе «iBank 2» в соответствии с действующими требованиями законодательства и Банка.

6.10. 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 «iBank 2». 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 «iBank 2», должен быть ограничен.

6.11. Клиент обязан по требованию Банка прекратить использовать указанный Банком ключ ЭП, сгенерировать новые ключи ЭП и зарегистрировать новый Сертификат ключа проверки ЭП в Банке.

6.12. Клиент обязан обеспечить хранение документов, составленных в электронном виде, в течение сроков, установленных действующим законодательством РФ. Документы, подписанные электронной подписью, практическая необходимость в которых отпала, и установленные сроки, хранения которых истекли, могут быть уничтожены.

6.13.Клиент обязан сформировать ЭП для каждого из уполномоченных лиц, указанных им в карточке с образцами подписей и оттиска печати, имеющейся в Банке. При этом, ЭП для каждого из уполномоченных лиц создается на отдельном USB токене.

6.13.1. Клиент имеет право сформировать дополнительную ЭП на отдельном USB токене, предназначенную для доступа в систему «iBank 2» 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 образцом подписи и оттиска печати, имеющейся в Банке, или для иного лица, полномочия которого подтверждены доверенностью в соответствии с действующим законодательством.

6.14. Клиент обязан сгенерировать новый ключ ЭП при изменении лиц, уполномоченных распоряжаться счетом(-ами), а также при Компрометации ключа ЭП.

6.15. По предложению Банка вносить необходимые изменения в программное и техническое обеспечение для работы системы «iBank 2».

6.16. 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 настоящих Правил.

6.17. Клиент имеет право по своему усмотрению генерировать новые ключи ЭП и регистрировать их в Банке.

6.18. Клиент имеет право, позвонив по телефону в Банк, и произнеся Блокировочное слово временно блокировать свою работу в системе «iBank 2». Такая устная блокировка должна сопро-

вождаться предоставлением письменного уведомления (Приложение № 5 к настоящим Правилам) в течение рабочего дня, следующего за днем блокировки.

6.19. Клиент имеет право возобновить свою работу в системе «iBank 2», которая ранее была заблокирована по инициативе Клиента, представив в Банк Заявление на возобновление предоставления ДОБС (Приложение № 7 к настоящим Правилам), заверенное оттиском печати, и подписями уполномоченных лиц Клиента, в соответствии с имеющейся в Банке карточке с образцами подписей и оттиска печати.

6.20. Клиент имеет право представить в Банк Заявление на IP-фильтрацию (Приложение № 10 к настоящим Правилам) и воспользоваться соответствующей услугой Банка.

6.21. Клиент имеет право представить в Банк Заявление на использовании MAC токена (Приложение № 11 к настоящим Правилам) и воспользоваться соответствующей услугой.

6.22. 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. 5.15. настоящих Правил.

6.23. Клиент обязан внимательно ознакомиться и выполнять требования «Инструкции по обеспечению информационной безопасности в системе ДОБС» (Приложение №12 к настоящим Правилам).

7. Размер и порядок оплаты услуг Банка

7.1. Клиент обязан оплачивать услуги Банка по предоставлению ДОБС, получению USB, MAC токенов по ставкам и в порядке, предусмотренном в действующих Тарифах Банка.

7.2. В случае неоплаты или неполной оплаты услуг Банка в течение 2-х недель, Банк направляет Клиенту уведомление (Приложение №4 к настоящим Правилам) посредством системы «iBank 2» и прекращает предоставлять Клиенту ДОБС.

7.3. Указанная в п.7.1. настоящих Правил плата, списывается Банком с любого счета Клиента, открытого в Банке, в безакцептном порядке. 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 РФ может быть квалифицирован как договор банковского счета / вклада.

8. Обязательства и ответственность сторон

8.1. За неисполнение или ненадлежащее исполнение предусмотренных настоящим Соглашением обязательств Стороны несут ответственность, предусмотренную действующим законодательством РФ, за исключением возмещения упущенной выгоды.

8.2. При расторжении Договора Стороны несут ответственность по всем электронным документам с активным ключом ЭП, сформированным в системе «iBank 2», до момента такого расторжения.

8.3. 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 «iBank2» Клиента.

8.4. 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.

8.5. 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.

8.6. Клиент несет риск убытков, которые могут возникнуть у него в результате несанкционированного использования его программно-технических средств системы «iBank2» и его ЭП, в том числе последствий воздействия на эти средства вредоносного кода.

8.7. Клиент несет ответственность за все действия, произведенные с использованием системы «iBank 2» от его имени и с использованием ЭП его уполномоченных лиц.

8.8. 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 настоящим Правилам).

8.9. 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.
8.10. При отмене использования документов в электронной форме документы, указанные в п.3.1. настоящих Правил, должны представляться Клиентом в Банк на бумажных носителях в общем порядке.
8.11. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием электронной системы «iBank 2», предоставлять в письменном виде свои оценки, доказательства и выводы.
8.12. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по настоящим Правилам 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.

9. Срок действия Договора

9.1. 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.
9.2. Стороны вправе расторгнуть Договор, причем такое расторжение вступает в действие с начала операционного дня рабочего дня, следующего за днем направления уведомления о расторжении Договора по системе «iBank2».
9.3. Договор считается автоматически расторгнутым, если в результате расторжения Договоров банковского счета, у Клиента не осталось ни одного Счета в Банке.

10. Общий порядок разрешения споров

10.1. 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-ти рабочих дней.
10.2. В случае возникновении спорных ситуаций между Клиентом и Банком при использовании электронной системы «iBank 2» Стороны обязуются участвовать в рассмотрении споров в соответствии с ст.11 настоящих Правил. При этом обмен электронными документами между Сторонами прекращается.
10.3. Если Стороны не смогут урегулировать возникшие разногласия в претензионном порядке, спор подлежит передаче на рассмотрение в Арбитражный суд г. Москвы.
10.4. Электронные документы, подписанные электронной подписью, допускаются в качестве письменных доказательств. Электронный документ отображается на бумажном носителе путем его распечатки.

11. Процедура разрешения спорных ситуаций

11.1. 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.
11.2. Клиент представляет Банку заявление, содержащее существо претензии с указанием на электронный документ, на основании которого Банк выполнил операции по счёту Клиента.

11.2.1. Заявление о несогласии с операцией рассматривается Банком в срок, не превышающий 30 календарных дней по Операциям, совершенным в Российской Федерации и в срок, не превышающий 60 календарных дней по Операциям, совершенным за пределами Российской Федерации.

11.3. Банк обязан в течение пяти дней от даты подачи заявления Клиента сформировать экспертную комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента и представители Банка. При необходимости в состав комиссии могут быть включены представители компании-разработчика системы «iBank 2» – ООО «Экспертно-Правовой Центр БИФИТ», а по специальному требованию одной из Сторон – независимые эксперты. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.

11.4. Стороны обязуются способствовать работе комиссии и не допускать отказа в предоставлении необходимых документов.

11.5. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых в системе.

11.6. В ходе работы комиссии каждая Сторона обязана доказать, что она исполнила обязательства по Договору надлежащим образом.

11.7. Результатом рассмотрения спорной ситуации экспертной комиссией является определение Стороны, несущей ответственность согласно выводу о подлинности ЭП Клиента под приложенным документом.

11.8. Экспертная комиссия в течение не более пяти дней проводит рассмотрение заявления. Рассмотрение заявления включает следующие этапы:

11.8.1. Экспертная комиссия проводит техническую экспертизу подлинности используемого ключа (ключей) ЭП Клиента.

11.8.1.1. С использованием системы «iBank 2» выполняется распечатка Сертификата ключа проверки ЭП Клиента (Приложение № 8 к настоящим Правилам).

11.8.1.2. Результат сверяется с Сертификатом ключа проверки ЭП (Приложение № 8 к настоящим 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.

11.8.2. Экспертная комиссия проводит техническую экспертизу электронного документа, заверенного необходимым количеством соответствующих ЭП Клиента, на основании которого Банком выполнены оспариваемые Клиентом действия.

11.8.3. Экспертная комиссия проводит техническую экспертизу подлинности ЭП Клиента в электронном документе.

11.8.3.1. Посредством системы «iBank 2» выбирается документ и выполняется операция «Проверить ЭП».

11.8.3.2. При невозможности получить доступ к документу через систему «iBank 2», могут использоваться специализированные утилиты от разработчика «iBank 2» для выгрузки документа из базы данных и автономной проверки.

11.8.4. На основании данных технической экспертизы экспертная комиссия составляет акт, содержащий:

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

11.8.5. 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 настоящим Правилам), подписанное должностным лицом Банка и имеющим оттиск пе-

чати Банка. При этом указанная в Уведомлении дата окончания действия ключей ЭП Клиента раньше даты, указанной в оспариваемом электронном документе.

11.9. В случае, когда Банк предъявляет электронный документ, подлинность ЭП Клиента в котором признана экспертной комиссией, и подтверждена принадлежность ключей ЭП Клиента, которыми подписан оспариваемый документ Банк перед Клиентом по выполненным операциям со счётом Клиента ответственности не несёт.

11.10. Если сторона Клиента настаивает на том, что данный документ она не создавала или не подписывала одной или несколькими электронными подписями, комиссия может вынести определение о компрометации ключа (ключей) ЭП Клиента, что не снимает ответственности Клиента за данный документ.

11.11. Если по проведенной проверке подлинности ЭП в оспариваемом документе, с ключом ЭП, предъявляемой Стороной, получившей оспариваемый документ, ЭП признана подлинной, то авторство оспариваемого электронного документа признается комиссией установленным.

11.12. Если по проведенной проверке подлинности ЭП в оспариваемом документе, с ключом ЭП, предъявляемой Стороной, получившей оспариваемый документ, ЭП не признана подлинной, то предъявленный для проверки авторства электронный документ признается комиссией ложным.

11.13. Претензии инициатора спора к противоположной Стороне признаются необоснованными, если инициатор спора был обязан в соответствии с настоящей Процедурой предъявить, но не предъявил комиссии полученный им файл, содержащий оспариваемый документ, или не предъявил Сертификат ключа проверки электронной подписи противоположной Стороны.

11.14. Отсутствие на клиентском рабочем месте системы «iBank 2» признаков отправки электронного документа, принятого Банком с подлинной ЭП данного Клиента, не является основанием для отказа Клиента от авторства данного документа.

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

ПРИЛОЖЕНИЕ № 1 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ДИСТАНЦИОННОЕ ОБСЛУЖИВАНИЕ БАНКОВСКИХ СЧЕТОВ

Полное наименование корпоративного клиента

_____

_____

Просим ПАО «МОСКОМБАНК», почтовый адрес: 119146, г. Москва, ул. 1-я Фрунзенская, д. 5 (далее – Банк), предоставить дистанционное обслуживание указанных ниже банковских счетов в Вашем Банке через интернет-соединение.

А также:

☐ - выдать USB-токен в количестве штук;

☐ - выдать MAC-токен в количестве штук.

Просим рассматривать настоящее Заявление как наш акцепт «Правил дистанционного обслуживания банковских счетов ПАО «МОСКОМБАНК» для корпоративных клиентов», с которыми мы ознакомлены, понимаем, полностью согласны, к которым мы присоединяемся полностью без каких-либо оговорок и изъятий, и которые обязуемся выполнять.

В соответствии с п. 2.2. указанных Правил договор, образованный Правилами и Заявлением, является неотъемлемой частью всех договоров банковского счёта, заключённых между Банком и Клиентом, а также договоров банковского счёта, которые могут быть заключены Сторонами в будущем. По заявлению Клиента некоторые договоры банковского счета, заключенные между Банком и Клиентом могут быть исключены из указанного общего правила.

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

В соответствии с «Правилами дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК», а также их акцептом настоящим Заявлением, а вместе образующих Договор, подключить Клиента к дистанционному обслуживанию указанных выше банковских счетов.

Уполномоченный сотрудник Банка _____ фамилия, инициалы | _____ подпись

						2	0		

М.П.

ПРИЛОЖЕНИЕ № 2 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

УВЕДОМЛЕНИЕ ОБ ОТМЕНЕ ДЕЙСТВИЯ КЛЮЧЕЙ ЭП

Полное наименование корпоративного клиента

_____

_____

На основании п.6.16 «Правил дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК» для корпоративных клиентов» уведомляем ПАО «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 ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 3 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

Минимальные системные требования

Для работы с системой «iBank2» необходимо:

1. Компьютер:
- Процессор – не хуже Intel Pentium 166 MHz ;
- Оперативная память - не менее 256 Mb;
- Операционная система - Windows XP/Vista/7/8;
- USB-порт.

2. Дополнительное оборудование:
- принтер.

3. Программное обеспечение:

- Java-машина (Java Runtime Environment);
- Web-браузер: Microsoft Internet Explorer, Mozilla Firefox; Opera, Google Chrome.

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 4 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДОБС

Полное наименование корпоративного клиента

_____

_____

На основании п.7.2 «Правил дистанционного обслуживания банковских счетов ПАО «МОСКОМБАНК» для корпоративных клиентов», уведомляем Вас о том, что с «__ __»_____20__ __г. дистанционное обслуживание Ваших банковских счетов будет приостановлено в связи с неоплатой или неполной оплатой услуг Банка по дистанционному обслуживанию банковских счетов.

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 5 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

ЗАЯВЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДОБС

Полное наименование корпоративного клиента

_____

_____

На основании п.8.8. «Правил дистанционного обслуживания банковских счетов ПАО «МОСКОМБАНК» для корпоративных клиентов» просим Вас прекратить предоставление дистанционного обслуживания наших банковских счетов на указанном ниже условии:

☐ - на период до ;

☐ - считать Договор о дистанционном обслуживании банковских счетов расторгнутым.

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 6 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА УСТАНОВКУ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Полное наименование корпоративного клиента

_____

_____

На основании п.6.1 «Правил дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК» для корпоративных клиентов» просим Вас установить программное обеспечение, необходимое для дистанционного обслуживания наших банковских счетов силами специалистов Банка. Предусмотренные Тарифами Банка комиссии обязуемся оплатить. Установка будет производиться:

☐ - на нашей территории по адресу ;

☐ - на территории Банка.

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	**0**		

Программное обеспечение установлено. Претензий не имеем.

Должность уполномоченного лица Клиента	фамилия, инициалы	подпись

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 7 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ПРЕДОСТАВЛЕНИЯ ДОБС

Полное наименование корпоративного клиента

_____

_____

На основании п.6.19 «Правил дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК» для корпоративных клиентов» просим Вас снять блокировку с нашей работы в системе «iBank2» и возобновить предоставление ДОБС.

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 8 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

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 ПАО «МОСКОМБАНК»
Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 9 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

АКТ ПРИЕМА-ПЕРЕДАЧИ

Полное наименование корпоративного клиента

_____

_____

На основании п.6.4.3. «Правил дистанционного обслуживания банковских счетов в ПАО «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	

В соответствии с п.6.4.3. вышеуказанных Правил 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 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

Полное наименование корпоративного клиента

_____

_____

На основании п.6.20 «Правил дистанционного обслуживания банковских счетов ПАО «МОСКОМБАНК» для корпоративных клиентов» просим Вас:

☐ - отменить ранее установленные ограничения;

☐ - установить возможность доступа в системе «iBank 2» 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.

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

МОСКОМБАНК
Commercial Bank of Moscow

ПРИЛОЖЕНИЕ № 11 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

ЗАЯВЛЕНИЕ НА ИСПОЛЬЗОВАНИЕ МАС ТОКЕНА

Полное наименование корпоративного клиента

_____

_____

На основании п.6.21 «Правил дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК» для корпоративных клиентов» просим Вас, для следующих МАС токенов:

№ п/п	Идентификатор токена
1	
2	
3	
4	
5	

☐ - установить дополнительную идентификацию одноразовым цифровым кодом при подключении к системе «iBank 2» с помощью МАС токена;

☐ - отменить ранее установленную дополнительную идентификацию одноразовым цифровым кодом при подключении к системе «iBank 2» с помощью МАС токена/OTP токена (нужное подчеркнуть);

☐ - установить дополнительное подтверждение одноразовым цифровым кодом при совершении платежей свыше руб.;

☐ - отменить ранее установленное дополнительное подтверждение одноразовым цифровым кодом при совершении платежей;

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

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

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	0		

Отметки ПАО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы	подпись

						2	0		

ПРИЛОЖЕНИЕ № 12 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ДОБС

В целях обеспечения информационной безопасности при работе в системе дистанционного обслуживания банковских счетов «iBank2» (далее – Система) **Клиент обязуется**:

1. Осуществлять вход в Систему только через корпоративный сайт ПАО «МОСКОМБАНК» *москомбанк.рф* (https://www.moscombank.ru).
2. 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 телефону (495) 609 19 19 доб.511. 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 «iBank 2».
3. Не отлучаться от компьютера, пока в нем находится USB токен или другой носитель, содержащий ключ электронной подписи.
4. Извлекать из компьютера USB токен или другой носитель, содержащий ключ электронной подписи, сразу после завершения работы 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. 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 телефону: (495) 609 19 19 доб.511, 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.

9. Обеспечивать конфиденциальность использования пароля Клиента для доступа к ключу ЭП; пароль не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы в работоспособном состоянии.
10. Применять на рабочем месте лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, спам-фильтры и т.п.
11. Производить периодическую (не реже 1 раза в 3 месяца) смену пароля ключей ЭП, а так же в случае компрометации или по требованию Банка.
12. Самостоятельно настроить используемое оборудование и программное обеспечение для работы с сетью Интернет по защищенному протоколу htpps.
13. Не использовать на рабочем месте любые средства удалённого (дистанционного) доступа, которые обычно практикуют IT-специалисты для удалённой (дистанционной) поддержки (TeamViewer и др.). Заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

Помимо указанных выше требований Банк настоятельно рекомендует:

1. Выделить для использования в Системе Банк-Клиент 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.
2. 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.
3. 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.
4. Перед началом работы проверить наличие защищенного (зашифрованного) соединения с сервером системы: символ замка и буква «S» в адресной строке – https://www.moscombank.ru, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.
5. Не использовать в качестве пароля простые, легко угадываемые комбинации букв и цифр, имена, фамилии, даты рождения и т.д., не записывать его там, где доступ к нему могут получить посторонние.
6. В качестве дополнительной меры по обеспечению информационной безопасности использовать MAC токен. Использование одноразовых цифровых кодов позволяет в системе «iBank 2» дополнительно идентифицировать Клиента, подтверждать платежи больше лимита и вести список доверенных получателей электронных платежей.
7. 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.
8. Для хранения ключей ЭП использовать только аппаратное средство хранения и генерации ключей ЭП – USB токен(ы) или другие средства, которые Банк примет решение применять для повышения безопасности платежей Клиентов.
9. 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 во время работы в Системе Банк-Клиент.
10. 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).

ПРИЛОЖЕНИЕ № 13 к
Правилам дистанционного обслуживания
банковских счетов ПАО «МОСКОМБАНК»
для корпоративных клиентов

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ОТКЛЮЧЕНИЕ ДИСТАНЦИОННОГО ОБСЛУЖИВАНИЯ НЕКОТОРЫХ БАНКОВСКИХ СЧЕТОВ

Полное наименование корпоративного клиента

_____

_____

Просим ПАО «МОСКОМБАНК», почтовый адрес: 119146, г. Москва, ул. 1-я Фрунзенская, д. 5 (далее – Банк), отключить дистанционное обслуживание указанных ниже наших банковских счетов в Вашем Банке:

Номер счета	**4**	**0**	**7**	**0**	**2**	**8**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Номер счета	**4**	**0**	**7**	**0**	**2**	**8**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Номер счета	**4**	**0**	**7**	**0**	**2**	**8**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Уполномоченные лица:

Должность	Фамилия, инициалы	Подпись
Должность	Фамилия, инициалы	Подпись

М.П.

						2	**0**		

Отметки ПАО «МОСКОМБАНК»

В соответствии с «Правилами дистанционного обслуживания банковских счетов в ПАО «МОСКОМБАНК отключить дистанционное обслуживание указанных выше банковских счетов Клиента.

Уполномоченный сотрудник Банка _____ | _____

фамилия, инициалы | подпись

						2	0		

М.П.