УТВЕРЖДЕНЫ
Правлением АО «МОСКОМБАНК»
Протокол № 01-05/26 от 11.09.2017 г.
Введено в действие с 14.09.2017 г.
Приказом № 01-08/65 от 11.09.2017 г.

МОСКОМБАНК
Commercial Bank of Moscow

ПРАВИЛА
дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» (версия 2.1)

Москва
2017

1. Определения

Банк – АО «МОСКОМБАНК»;
Клиент – частный клиент Банка – физическое лицо, не осуществляющее предпринимательской или инвестиционной деятельности;
Сторона, Стороны – Банк и/или Клиент;
Счет – банковский счет, в том числе специальный карточный счет Клиента, открываемый Банком на имя Клиента на основании договора;
Электронный банк – электронное средство платежа, то есть способ, позволяющий Клиенту составлять, удостоверять и передавать в Банк распоряжения в целях осуществления перевода денежных средств, а также предоставлять Клиенту информацию о совершенных операциях с использованием информационно-коммуникационных технологий и/или электронных носителей информации;
АБС – автоматизированная банковская система, обеспечивающая посредством Электронного банка, получение распоряжений в целях осуществления перевода денежных средств, проверку их авторства, подлинности и целостности, осуществление переводов денежных средств, а также передачу информации о совершенных операциях;
Распоряжение – сообщение или несколько связанных сообщений в виде Электронных документов, содержащих указание Клиента Банку о совершении соответствующей операции, составленное и переданное посредством Электронного банка;
Электронный документ (ЭД) – совокупность информации в цифровой форме, содержащая финансовый документ, информационное или служебное сообщение в Электронном банке;
Информационный сервис – предоставление Клиенту возможности получения посредством Электронного банка актуальной и достоверной информации о состоянии Счетов, дополнительной информации, а также сервисных и других операциях, доступных в Электронном банке;
Правила – настоящие «Правила дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК»;
Заявление – Заявление на дистанционное банковское обслуживание (далее – ДБО), направляемое Клиентом Банку;
Договор – договор о дистанционном банковском обслуживании, образованный Правилами, являющимися публичной офертой Банка и акцептованные Клиентом посредством должным образом подписанного и оформленного Заявления;
Идентификаторы учетной записи Клиента – уникальная пара цифровой информации (логин и пароль), многократно используемая для аутентификации Клиента в Электронном банке и однозначно выделяющая (идентифицирующая) Клиента среди определенного множества клиентов Банка;
Аутентификация – процедура проверки подлинности вводимых идентификаторов учетной записи путем сравнения введенного Пароля, Одноразового пароля с хранящимся в базе данных Банка и сопоставления их введенному Логину Клиента;
Пароли доступа – общее название всех паролей Клиента, используемых при работе с Электронным банком. К паролям доступа относятся долговременный пароль учетной записи Клиента, пароль для доступа к секретному ключу ЭП, одноразовый пароль, отправляемый в СМС-сообщении, одноразовый пароль, генерируемый OTP-токеном, и т.д.;
Одноразовый пароль – уникальный случайно образованный одноразовый набор символов, направляемый Клиенту на Зарегистрированный номер телефона в виде СМС-сообщения или генерируемый OTP-токеном. Каждый сформированный АБС Одноразовый пароль имеет ограниченный срок действия, который устанавливается/изменяется Банком с учетом требований к информационной безопасности при обслуживания Клиентов. Одноразовый пароль может быть использован только один раз. Все операции, совершенные с использованием Одноразового пароля, считаются совершенными от имени Клиента и с его согласия;
СМС-сообщение (уведомление) – сообщение, сформированное АБС и отправленное через оператора подвижной сотовой радиотелефонной связи Клиенту на его Зарегистрированный телефонный номер;

Зарегистрированный телефонный номер – телефонный номер, обслуживаемый оператором подвижной сотовой радиотелефонной связи, оформленный на имя Клиента и зарегистрированный в Электронном банке для отправки Банком Клиенту Идентификаторов учетной записи и одноразовых паролей, посредством СМС-сообщений.

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 (Клиента), подписывающего информацию;

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Клиентом;

Усиленной неквалифицированной электронной подписью является электронная подпись, которая:

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

Ключ ЭП Клиента – ключ (уникальная последовательность символов), самостоятельно генерируемый Клиентом с использованием средств Электронного банка, 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 Электронного банка, 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 подписью Клиента или его уполномоченных лиц и оттиском печати Клиента (при наличии) в соответствии с карточкой с образцами подписей и оттиска печати, имеющейся в Банке;

Активный ключ ЭП Клиента – ключ ЭП Клиента, зарегистрированный Банком в АБС и используемый Клиентом для работы;

Средство криптографической защиты информации (СКЗИ) – СКЗИ «КриптоПро CSP» (версии 3.6) компании ООО «КРИПТО-ПРО», входящее в состав Электронного банка и АБС и имеющее сертификаты ФСБ России СФ/114-2237, СФ/124-2238 от 04.10.2013 г., СФ/121-2271, СФ/121-2272 от 12.12.2013 г., СФ/124-2503 СФ/124-2504 от 12.02.2015 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 криптографические алгоритмы и имеется защищенная область памяти, позволяющее генерировать и безопасно хранить ключи ЭП;

OTP-токен – аппаратное устройство, предназначенное для генерации одноразовых паролей.

АСП – аналог собственноручной подписи – простая электронная подпись, которая посредством использования идентификационной пары (логина и пароля) и одноразового пароля подтверждает факт формирования электронной подписи Клиентом и используется для подтверждения авторства электронного документа;

Подлинный АСП – АСП, подлинность которого проверена и подтверждена программно-аппаратными средствами АБС;

Подтверждение распоряжения – процедура, основанная на использовании одноразовых паролей, целью которой является контроль подлинности, неизменности и целостности Распоря-

жения, подтверждение авторства Клиента в отношении Распоряжения при его принятии, и/или получение Банком юридически значимого доказательства авторства Клиента;

Компрометация ключа ЭП – 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);

Компрометация Пароля – событие, в результате которого доступ к Паролю получили, либо могли получить, неуполномоченные лица;

Подлинность электронного документа означает, что данный документ создан в Электронном банке 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 пользователем Электронного банка;

Безотзывность перевода денежных средств – характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств в определенный момент времени; время наступления безотзывности перевода наступает в момент списания денежных средств Клиента;

Протокол соединения – Электронный документ, подтверждающий факт передачи Клиентом Распоряжения, в том числе запись сеанса связи, сделанная при помощи записывающего устройства, или протокол сеанса связи в виде совокупности записей в базе данных АБС;

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 АБС, Электронный банк, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование пользователей Электронного банка, 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;

IP-фильтрация - фильтрация IP адресов, позволяющая осуществлять вход в Электронный банк только с определенных компьютеров (мобильных устройств). Используется для повышения информационной безопасности при работе в Электронном банке 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.

2. Общие положения

2.1. Настоящие Правила определяют порядок предоставления Банком дистанционного обслуживания Клиентам с помощью Электронного банка, который позволяет получать дистанционный доступ к банковским счетам, составлять электронные распоряжения на перевод денежных средств, принимать выписки по банковским счетам, а также передавать и принимать различные Электронные документы.

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

2.3. Заявление Клиента и настоящие Правила, к которым Клиент присоединяется полностью и без каких-либо изъятий образуют Договор.

2.4. Доступ к Электронному банку предоставляется по Заявлению Клиента, в том числе, направленному в Банк в электронной форме в процессе электронной регистрации.

2.5. Клиент подтверждает, что до присоединения к настоящим Правилам ознакомился и проинформирован об условиях использования Электронного банка, в частности о любых ограничени-

ях способов и мест использования, случаях повышенного риска его использования как электронного средства платежа.
2.6. Электронный банк предоставляется Клиенту через вэб-интерфейс к АБС и/или специальное приложение, которое может быть установлено на мобильное устройство из интернет-магазинов App Store или Google Play.
2.7. Взаимодействие Электронного банка и АБС осуществляется с использованием информационно-телекоммуникационной сети Интернет (далее – сеть Интернет), к которой должно быть подключено устройство Клиента, на котором используется Электронный банк.
2.8. Состав и содержание сервисов Электронного банка, доступных Клиенту, определяется Банком и может меняться им по своему усмотрению и без предварительного уведомления.

3. Доступ к Электронному банку

3.1. Доступ к Электронному банку предоставляется при наличии технической возможности круглосуточно с использованием сети Интернет, исключая технические перерывы, о которых сообщается отдельно. Техническая поддержка Клиентам предоставляется в рабочие часы Банка.
3.2. Для получения доступа, Клиенту необходимо:

- Запустить Электронный банк с сайта Банка москомбанк.рф (www.moscombank.ru);
- Или перейти по интернет-ссылке https://mypay.moscombank.ru;
- Или воспользоваться мобильным приложением, установив его на свое мобильное устройство с магазинов AppStore или GooglePlay.

3.3. Для получения доступа к Электронному банку с возможностью просмотра информации по счетам, банковским картам, вкладам и кредитам, другой информации Банка, а также с возможностью составления Распоряжений на перевод денежных средств, Клиенту необходимо лично представить в Банк заявление (Приложение № 1 к настоящим Правилам).
3.4. Клиент – держатель банковской карты АО «МОСКОМБАНК» может пройти электронную регистрацию без личной подачи заявления. В этом случае, ему предоставляется краткий Информационный сервис к сведениям о счетах и остатках денежных средств на них без возможности направления в Банк распоряжений на перевод денежных средств.
3.4.1. Клиент, прошедший только электронную регистрацию может в дальнейшем расширить свои права, представив в Банк заявление в порядке, аналогичном п. 3.3.
3.5. Для подтверждения доступа в Электронный банк, направления в Банк распоряжений на перевод денежных средств, в иных случаях, установленных Банком, используются одноразовые пароли, направляемые Клиенту в виде СМС-сообщения (SMS-сообщения) на его Зарегистрированный телефонный номер либо генерируются OTP-токеном Клиента
3.6. Для подтверждения доступа в Электронный банк через мобильные устройства может использоваться дополнительная идентификация Клиента посредством PIN-кода, который привязывается к конкретному мобильному устройству Клиента.

4. Документы

4.1. Стороны договорились использовать в электронной форме документы, предусмотренные законодательством РФ, нормативными актами Банка России и Банка, регулирующие осуществление безналичных расчетов в РФ.
4.2. По требованию Банка Клиент обязан в двухдневный срок предоставить на бумажном носителе экземпляр любого документа, указанного в п. 4.1. Правил, им подписанного, в соответствии с карточкой с образцами подписей, имеющейся в Банке.
4.3. Документы, указанные в п. 4.1. настоящих Правил, изготавливаются в электронной форме на основе использования предоставляемого Банком программного обеспечения Электронного банка. Форматы документов в электронной форме формируются Электронным банком.
4.5. Отображение электронного документа на бумажном носителе осуществляется путём его распечатки на принтере исключительно через Электронный банк.
4.6. Подлинником электронного документа является электронный образ документа в оговоренном формате, который содержит текст документа, АСП или ЭП Клиента, подписавшего этот документ, с положительным результатом проверки подлинности ЭП, произведенной программ-

ными средствами АБС, с использованием ключей проверки ЭП, зарегистрированных в установленном Правилами порядке. Результаты проверки подлинности фиксируются с использованием программных средств АБС.

5. Соглашения Сторон

5.1. Стороны признают, что:
5.1.1. используемый в Электронном банке механизм аутентификации является достаточной мерой защиты от доступа третьих лиц к информации по банковским счетам Клиента.
5.1.2. использование АСП или ЭП является достаточной мерой подтверждения Подлинности и Авторства электронных документов.
5.1.3. использование USB-токена является необходимым средством защиты ключа ЭП, если Клиент использует ЭП.
5.1.4. использование IP-фильтрации является дополнительной мерой защиты при идентификации Клиента.
5.1.5. Риск неправомерного использования ЭП или АСП Клиента третьими лицами несет Клиент. Клиент заявляет о признании подлинности и надлежащего подписания всех документов, заверенных ЭП или АСП, пока официально не будет объявлено о Компрометации ключа ЭП или АСП.
5.2. В соответствии с положениями Федерального Закона РФ «Об электронной подписи» № 63-ФЗ от 06 апреля 2011 года используемая в Электронном банке электронная подпись на основе российских криптоалгоритмов признается сторонами усиленной неквалифицированной ЭП, а используемые коды, пароли или иные средства (в том числе, направляемые посредством СМС-сообщений на Зарегистрированный телефонный номер Клиента), подтверждающие факт формирования электронной подписи определенным лицом, признаются сторонами простой ЭП.
5.2.1. Клиент обязан использовать для хранения ключей ЭП USB-токены. В этом случае обеспечивается их неизвлекаемость (неэкспортируемость).
5.3. Стороны признают, что при произвольном изменении электронного документа, заверенного ЭП, целостность ЭД нарушается, то есть проверка ЭП дает отрицательный результат.
5.4. Стороны признают, что подделка ЭП или АСП Клиента, то есть создание подлинной ЭП или АСП электронного документа от имени Клиента, невозможна без обладания ключом ЭП Клиента или знания идентификационных кодов, паролей, позволяющих формировать электронную подпись (АСП) определенным лицом.
5.5. Стороны признают, что электронные документы, заверенные ЭП или АСП, 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 ЭП или АСП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.
5.6. Стороны признают, что электронные документы с ЭП или АСП Клиента, создаваемые в АБС, являются доказательным материалом для решения спорных вопросов в соответствии с «Порядком разрешения спорных ситуаций» Раздела 11 Правил. Электронные документы, не имеющие ЭП или АСП, при наличии спорных вопросов, не являются доказательным материалом.
5.7. Стороны признают, что ключ проверки ЭП Клиента, указанный в заверенном собственноручной подписью Клиента Сертификате ключа проверки ЭП Клиента (Приложение № 8 к настоящим Правилам), принадлежит Клиенту.
5.8. Стороны признают в качестве единой шкалы времени при работе с АБС Московское поясное время. Контрольным является время системных часов АБС.

6. Права и обязанности Банка

6.1. Банк может предоставлять Клиенту для генерации одноразовых паролей OTP-токены, необходимые для хранения ЭП USB-токены, а также обеспечивает гарантированную доступность

Электронного банка в сети Интернет согласно п.3.1 в рабочие часы Банка, исключая технические перерывы, о которых сообщается отдельно.
6.2. 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.
6.2.1. Электронные документы, которые могут быть приняты, проверены, обработаны и исполнены без привлечения сотрудников Банка в автоматическом режиме, исполняются незамедлительно.
6.3. При получении Электронного документа Банк производит проверку подлинности ЭП или АСП Клиента, проверку правильности заполнения реквизитов ЭД, проверку на возможность возникновения дебетового сальдо на счёте Клиента. Банк принимает к исполнению только Электронные документы, имеющие положительный результат выполнения вышеуказанных процедур.
6.4. Банк обязуется по требованию Клиента блокировать в АБС учетную запись Клиента или активные ключи ЭП Клиента. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.
6.5. Банк обязан возобновить возможность работы Клиента в Электронном банке, разблокировав в АБС учетную запись Клиента, только при поступлении от Клиента соответствующего заявления (Приложение № 6 к настоящим Правилам), заверенного собственноручной подписью Клиента.
6.6. Банк обязан хранить принятые от Клиента данные с АСП или ЭП в течение пяти лет.
6.7. При наличии подозрений о компрометации учетной записи Клиента, ключа ЭП Клиента или неправильном их использовании Банк имеет право по своему усмотрению, без уведомления Клиента блокировать учетную запись Клиента или активный ключ ЭП Клиента, и потребовать от Клиента их смены.
6.8. В случае нарушения Клиентом настоящих Правил, условий договора банковского счета, а также в иных аналогичных случаях Банк имеет право по своему усмотрению, без уведомления Клиента блокировать доступ Клиента к Электронному банку, не принимать к исполнению электронные документы.
6.9. При наличии подозрений о компрометации учетной записи Клиента, ключа ЭП Клиента или не правильном их 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.
6.10. Банк имеет право на внесение изменений в программное обеспечение Электронного банка по собственному усмотрению и без предварительного уведомления.
6.11. Банк имеет право на внесение изменений в Правила в одностороннем порядке. Новая редакция Правил вступает в действие через 15 календарных дней после уведомления Клиента. Уведомление Клиента осуществляется путем рассылки информационного сообщения в Электронном банке, размещения информации на сайте Банка москомбанк.рф (www.moscombank.ru), а также на информационных стендах в офисах Банка.
6.12. Банк информирует Клиента о совершении каждой операции с использованием Электронного банка путем направления Клиенту соответствующего уведомления одним или несколькими указанными ниже способами:
6.12.1. 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 АСП/ЭП электронного документа принято Электронным банком 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 рассмотрено специалистом Банка и поставлено в очередь на исполнение текущим днем;
- «Исполнено» - означает, что распоряжение направлено банку получателя платежа.

6.12.2. Путем предоставления Клиенту возможности получить в режиме реального времени информацию об остатке денежных средств на Счете, а также о последних операциях по Счету посредством специально сформированного запроса в Электронном банке;
6.12.3. Путем предоставления Клиенту возможности сформировать в режиме реального времени и распечатать выписку по Счету посредством специально сформированного запроса в Электронном банке;
6.12.4. Путем предоставления Клиенту возможности в период работы Банка получить выписку по Счету на бумажном носителе при его личном обращении в Банк.
6.12.5. 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.
6.13. Банк фиксирует направляемые Клиенту уведомления и хранит их в течение трех лет.

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 Электронном банке без получения собственной лицензии.
7.2. При конфигурации рабочих мест Клиент обязан учитывать требования, предъявляемые к конфигурации компьютера или мобильного устройства, его программному обеспечению, на котором производится использование Электронного банка (Приложение № 3 к настоящим Правилам), а также то, что несанкционированное изменение конфигурации может привести к сбою в работе Электронного банка.
7.3. Перед началом эксплуатации Электронного банка и при использовании ЭП Клиент обязан получить в Банке (скачать с сайта Банка) и самостоятельно установить на своем компьютере или мобильном устройстве СКЗИ, а также получить и использовать Токен, позволяющий генерировать и безопасно хранить ключи ЭП.
7.3.1. Для целей информационной безопасности Банк имеет право ограничивать применение СКЗИ на мобильных устройствах, если программные или аппаратные средства не позволяют их безопасно использовать.
7.4. Клиент обязуется использовать предоставленное СКЗИ только в Электронном банке, 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 Электронного банка, включая предоставленное Банком СКЗИ.
7.6. Клиент обязан сообщать Банку, не позднее следующего рабочего дня с момента обнаружения, о возникновении следующих ситуаций:

- несанкционированный доступ или попытка такого доступа к Электронному банку;
- совершение с помощью Электронного банка платежа без согласия Клиента;
- потеря, в том числе кратковременная, контроля над носителями секретного ключа ЭП или мобильного устройства, телефона сотовой радиотелефонной связи, на который направлялись СМС-сообщения, содержащие одноразовые пароли;
- компрометация ключей ЭП или логина и пароля для доступа к Электронному банку;
- отказ подтверждения программой проверки ЭП или АСП принимаемого электронного документа;
- возникновение ошибки при совершении электронных платежей.

7.6.1. Под ошибкой в целях 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;

7.6.2. Указанное в 7.6 сообщение Банку будет считаться надлежащим образом направленным,, если Клиент осуществит следующие действия:

- незамедлительно блокирует Ключ ЭП Клиента по телефону +7(495) 109-00-14;
- направит в Банк не позднее дня следующего за днем совершения платежа без согласия Клиента Заявление о несогласии с Операцией, установленного в Банке образца одним из следующих способов:
    - На бумажном носителе по факсу +7 (499) 242-82-19 с последующим предоставлением оригинала документа;
    - На бумажном носителе в офисах банка по рабочим дням в рабочее время Банка. Адреса офисов Банка указаны на Сайте.

7.7. Клиент обязан в случае прекращения использования Электронного банка удалить установленное на его компьютерах или мобильных устройствах программное обеспечение Электронного банка, включая СКЗИ.
7.8. Клиент обязан хранить в секрете и не передавать третьим лицам логины, пароли, Токены. Клиент обязан ограничить доступ третьих лиц к своему телефону подвижной сотовой радиотелефонной связи, на который Электронный банк направляет одноразовые пароли.
7.9. Клиент обязан по требованию Банка прекратить использовать указанный Банком ключ ЭП, сгенерировать новые ключи ЭП и зарегистрировать новый сертификат ключа проверки ЭП в Банке.
7.10. 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.
7.11. Клиент обязан сгенерировать новый ключ ЭП при Компрометации.
7.12. Клиент обязан обновлять программное обеспечение Электронного банка и СКЗИ по требованию Банка.
7.13. Клиент имеет право досрочно прекратить действие своей учетной записи и/или своего активного ключа ЭП и потребовать от Банка блокировать свою учетную запись и/или свой активный ключ ЭП, оформив уведомление по форме Приложения № 2 к Правилам.
7.14. Клиент имеет право по своему усмотрению сгенерировать новые ключи ЭП и зарегистрировать в Банке новые сертификат ключа проверки ЭП Клиента.
7.15. Клиент имеет право, позвонив по телефону в Банк временно блокировать свою работу в Электронном банке. Такая устная блокировка должна сопровождаться предоставлением письменного уведомления (Приложение № 5 к настоящим Правилам).
7.15.1. Такая блокировка возможна только при условии однозначной идентификации Клиента.
7.16. Клиент имеет право возобновить свою работу в Электронном банке, которая ранее была заблокирована по его инициативе, представив в Банк Заявление на возобновление предоставления дистанционного банковского обслуживания (Приложение № 6 к настоящим Правилам).
7.17. Клиент имеет право представить в Банк Заявление на IP-фильтрацию (Приложение № 7 к настоящим Правилам) и воспользоваться соответствующей услугой.
7.18. Клиент обязан внимательно ознакомиться и выполнять требования «Инструкции по обеспечению информационной безопасности в Электронном банке» (Приложение №10 к настоящим Правилам).
7.19. 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. 6.12. Правил.

8. Размер и порядок оплаты услуг Банка

8.1. Клиент обязан оплачивать услуги Банка по предоставлению доступа к Электронному банку, получению USB и OTP - токенов по ставкам и в порядке, предусмотренном в действующих Тарифах Банка.

8.2. В случае неоплаты или неполной оплаты услуг Банка в течение 2-х недель, Банк направляет Клиенту уведомление (Приложение № 4 к настоящим Правилам) посредством Электронного банка и прекращает предоставлять Клиенту услуг дистанционного обслуживания.
8.3. Указанная в п.8.1. 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.

9. Обязательства и ответственность сторон

9.1. За неисполнение или ненадлежащее исполнение предусмотренных настоящим Соглашением обязательств, Стороны несут ответственность, предусмотренную действующим законодательством РФ, за исключением возмещения упущенной выгоды.
9.2. При расторжении Договора Стороны несут ответственность по всем электронным документам с ЭП и АСП, сформированным с помощью Электронного банка, до момента такого расторжения.
9.3. Банк не несёт ответственности за ущерб, причинённый Клиенту в результате использования третьими лицами учетной записи Клиента, АСП Клиента, ключа ЭП Клиента.
9.4. Банк не несет ответственности за сбои в работе линий связи и провайдеров, технических средств, программного обеспечения, повлекшие для Банка невозможность предоставления доступа к Электронному банку в соответствии с п. 3.1. Правил, а для Клиента невозможность передачи платежного документа в электронной форме или получения информации о совершенных операциях.
9.5. Клиент несет риск убытков, которые могут возникнуть у него в результате несанкционированного использования его программно-технических средств, учетной записи, АСП и ЭП с учетом действующего законодательства.
9.6. 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).
9.7. 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.
9.8. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Электронного банка, предоставлять в письменном виде свои оценки, доказательства и выводы.
9.9. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых по 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.

10. Порядок обеспечения безопасности работы с Электронным банком

10.1. Использование Пароля.
10.1.1 Клиент может самостоятельно изменять Пароль путем выполнения предусмотренной в Электронном банке процедуры смены Пароля.

10.1.2 Клиент обязуется обеспечить хранение информации о Пароле способом, делающим Пароль недоступным третьим лицам, а также немедленно уведомлять Банк о Компрометации Пароля.
10.1.3 Клиент не должен сообщать Пароль сотрудникам Банка по телефону, электронной почте или иным способом. Использование Пароля допускается только при работе Клиента непосредственно с Электронным банком, без участия сотрудников Банка.
10.1.4. С целью повышения информационной безопасности при использовании Электронного банка с мобильных устройств, для входа в систему может использоваться PIN-код, который привязывается к конкретному мобильному устройству.
10.1.5. С целью минимизации риска Клиента, связанного с несанкционированным использованием Электронного банка третьими лицами, Банк может устанавливать ограничения (лимиты) на сумму операции или совокупный объем операций за определенный период, совершаемых Клиентом с использованием Электронного банка. Указанные ограничения устанавливаются Банком в зависимости от используемого Клиентом интерфейса (вэб-решение или приложение мобильного устройства).

10.2. Зарегистрированный номер телефона для СМС-сообщений.
10.2.1 В ходе самостоятельной регистрации в Электронном банке Клиент указывает номер личного телефона сотовой подвижной радиотелефонной связи для отправки СМС-сообщений. С момента регистрации в Электронном банке указанный номер телефона становится Зарегистрированным номером телефона для СМС-сообщений. Зарегистрированным номером телефона для СМС-сообщений может являться только один телефонный номер.
10.2.2 Клиент может изменить Зарегистрированный номер телефона для СМС-сообщений путем представления в Банк письменного Заявления об изменении Зарегистрированного номера телефона для СМС-сообщений, составленного по форме Приложения № 10 к настоящим Правилам.
10.2.3 Банк вправе без объяснения причин отказать Клиенту в регистрации в Электронном банке телефонного номера и/или в изменении Зарегистрированного номера телефона для СМС-сообщений.
10.2.4 Клиент обязуется исключить возможность использования иными лицами устройства, телефонный номер которого является Зарегистрированным номером телефона для СМС-сообщений, а также немедленно уведомлять Банк об утрате или возникновении риска несанкционированного использования такого устройства.

10.3. Использование одноразовых паролей.
10.3.1. Подтверждение Распоряжения с помощью одноразовых паролей осуществляется путем предоставления Клиенту уникального цифрового кода, произвольно сгенерированного АБС. Клиент сообщает Банку одноразовый пароль путем ввода принятого уникального цифрового кода в предназначенную для этой цели форму Электронного банка. Доставка одноразового пароля Клиенту может осуществляться двумя альтернативными методами:

- СМС-сообщением на Зарегистрированный номер телефона;
- Выводом пароля на экран OTP-токена.

10.3.2 Срок действия одноразового пароля, предоставленного Банком Клиенту, устанавливается Банком и указывается на экране Электронного банка при его генерации.
10.3.3 Положительный результат проверки одноразового пароля означает, что Распоряжение Клиента принято.
10.3.4 Клиент обязуется обеспечить хранение одноразовых паролей способом, делающим их недоступными третьим лицам.
10.3.5 Клиент не должен сообщать одноразовые пароли сотрудникам Банка по телефону, электронной почте или иным способом. Использование одноразовых паролей допускается только при работе Клиента непосредственно в Электронном банке, без участия сотрудников Банка.
10.3.6 Банк не несет ответственности за ущерб, возникший вследствие несанкционированного использования третьими лицами одноразовых паролей.
10.3.7 Банк не несет ответственности за неполучение Клиентом СМС-сообщений, содержащих одноразовые пароли, произошедшее не по вине Банка.

10.3.7.1. Электронный банк информирует Клиента об отправке СМС-сообщения. Клиент имеет возможность активировать повторную отправку СМС-сообщения в необходимых случаях.
10.3.8 Банк обязуется принять все необходимые меры организационного и технического характера для обеспечения режима конфиденциальности в отношении одноразовых паролей до передачи их в систему доставки для передачи Клиенту.

10.4. Конфиденциальность.
10.4.1 Банк обязуется принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Электронного банка.
10.4.2 Любая информация такого рода может быть предоставлена третьим лицам исключительно в порядке, установленном действующим законодательством РФ.
10.4.3 Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации по сети Интернет влечет риск несанкционированного доступа к такой информации третьих лиц.
10.4.4 В случае, когда передача информации по сети Интернет осуществляется по требованию или в соответствии с Распоряжением Клиента, Банк не несет ответственности за несанкционированный доступ третьих лиц к такой информации при ее передаче.

11. Срок действия Договора

11.1. Договор вступает в силу с момента (и/или):
- акцепта Банком Заявления Клиента, им подписанного в соответствии с имеющейся в Банке карточкой с образцами подписей и представленного в Банк лично Клиентом или его уполномоченными лицами;
- получения Банком Заявления в электронной форме, направленного средствами Электронного банка в порядке регистрации.

11.2. Договор заключается на неопределенный срок.
11.3. Стороны вправе расторгнуть Договор, причем такое расторжение вступает в действие с начала операционного дня рабочего дня, следующего за днем направления уведомления о расторжении Договора.
11.4. Договор считается автоматически расторгнутым, если в результате расторжения Договоров банковского счета, у Клиента не осталось ни одного Счета в Банке.

12. Общий порядок разрешения споров

12.1. 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.
12.2. В случае возникновении спорных ситуаций между Клиентом и Банком при использовании Электронного банка Стороны обязуются участвовать в рассмотрении споров в соответствии с разделом 13 Правил. При этом обмен электронными документами между Сторонами прекращается.
12.3. Если Стороны не смогут урегулировать возникшие разногласия в претензионном порядке, спор передается в судебные инстанции г. Москвы в зависимости от суммы требования, установленной законодательством: Мировому судье судебного участка № 366 района Хамовники г. Москвы (или иного судебного участка, к территориальной подсудности которого будет относиться адрес места нахождения АО «МОСКОМБАНК»: г. Москва, ул. 1-я Фрунзенская, д. 5) или в Хамовнический районный суд г. Москвы.
12.4. Электронные документы, подписанные ЭП или АСП, допускаются в качестве письменных доказательств. Электронный документ отображается на бумажном носителе путем его распечатки.

13. Процедура разрешения спорных ситуаций

13.1. Под спорной ситуацией понимается возникновение претензий у Клиента к Банку вследствие совершения посредством Электронного банка операции (платежа), на которую Клиент не давал согласия.
13.2. В случае такого несогласия Клиент представляет Банку Заявление о несогласии с операции в соответствии с п. 6.8.2.
13.3. Заявление о несогласии с операцией рассматривается Банком в срок, не превышающий 30 календарных дней а также в срок не более календарных 60 дней в случае осуществления Клиентом, посредством Электронного банка трансграничного перевода денежных средств.
13.3.1. Трансграничный перевод денежных средств – это перевод денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный банк.
13.4. По результатам рассмотрения Банком Заявления о несогласии с Операцией, Банк может принять решение:
13.4.1. О возмещении Клиенту суммы Операции, совершенной без согласия Клиента, если Клиентом не были нарушены Правила, в том числе в части выполнения Клиентом обязанности по получению уведомления о каждой совершенной операции (п. 6.22 Правил), в части выполнения Клиентом порядка направления в Банк Заявления о несогласии с Операцией и блокировки Ключа ЭП Клиента (п. 6.8.2, Правил), а также законодательство Российской Федерации.
13.4.2. О мотивированном отказе в возмещении Клиенту суммы, указанной в Заявлении о несогласии с Операцией.
13.5. Банк в течение пяти дней от даты подачи Заявления о несогласии с Операцией Клиента формирует экспертную комиссию для рассмотрения Заявления. В состав комиссии включаются представители Клиента и представители Банка, а по специальному требованию одной из Сторон – независимые эксперты. Состав комиссии должен быть зафиксирован в акте, который является итоговым документом, отражающим результаты работы комиссии.
13.6 . Стороны обязуются способствовать работе комиссии и не допускать отказа в предоставлении необходимых документов.
13.7. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных и аппаратных средств, используемых для работы в Электронном банке.
13.8. В ходе работы комиссии каждая Сторона обязана доказать, что она исполнила обязательства по Договору надлежащим образом.
13.9. Результатом рассмотрения спорной ситуации экспертной комиссией является определение Стороны, несущей ответственность согласно выводу о подлинности АСП или ЭП Клиента под приложенным документом.
13.10. Экспертная комиссия проводит техническую экспертизу подлинности АСП или ЭП Клиента в электронном документе. при этом проверяется, что:

- срок действия сертификата ключа ЭП не истек;
- Банк не имеет Уведомления об отмене действия в соответствии с Приложением № 2 к настоящим Правилам.

13.11. 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.

13.12. Если по проведенной проверке подлинности АСП или ЭП в оспариваемом документе, предъявляемой Стороной, получившей оспариваемый документ, ЭП признана подлинной, то авторство оспариваемого электронного документа признается комиссией установленным.
13.13. Если по проведенной проверке подлинности АСП или ЭП в оспариваемом документе, предъявляемой Стороной, получившей оспариваемый документ, ЭП не признана подлинной, то предъявленный для проверки авторства электронный документ признается комиссией ложным.

13.14. 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.
13.15. Претензии Клиента к Банку признаются необоснованными, если Клиент не предъявил свой Токен (в случае использования ключа ЭП).
13.16. По итогам работы комиссии составляется итоговый акт, подписываемый всеми членами комиссии.

МОСКОМБАНК
Commercial Bank of Moscow

Приложение № 1 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ В ЭЛЕКТРОННОМ БАНКЕ

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

Прошу АО «МОСКОМБАНК» (Лицензия Банка России № 3172 от 26.10.1999 г (далее – Банк), предоставить мне доступ к системе дистанционного обслуживания «Электронный банк» в режиме просмотра информации о моих счетах, картах, вкладах, кредитах, иной информации Банка без права составления распоряжений на перевод денежных средств.

Дополнительно прошу:

☐ - предоставить право в «Электронном банке» составлять, подписывать и направлять в Банк на исполнение электронные распоряжения на перевод денежных средств;
☐ - установить ограничение в «Электронном банке» на максимальную сумму распоряжения на перевод денежных средств в размере:

- рублей*, с использованием подтверждения одноразовым паролем;
- рублей*, с использованием токена с электронной подписью.

Прошу рассматривать настоящее Заявление, как мой акцепт «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК», с которыми я ознакомлен, понимаю, полностью согласен, к которым я присоединяюсь полностью без каких-либо оговорок и изъятий, и которые обязуюсь выполнять.

*) для валютных счетов будет применяться ограничение, рассчитанное по курсу Банка России на день совершения операции

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

В соответствии с «Правилами дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК», а также их акцептом настоящим Заявлением, а вместе образующих Договор, подключить Клиента к дистанционному обслуживанию в системе «Электронный банк».

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

М.П.

Приложение № 2 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

УВЕДОМЛЕНИЕ ОБ ОТМЕНЕ ДЕЙСТВИЯ

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

На основании п.6.16 «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК», уведомляю Вас о том, что с считается недействительным:

☐ - моя учетная запись в «Электронном банке» ;

☐ - ключ ЭП (OTP-токен) со следующим идентификатором .

Клиент

подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

«Принято к исполнению»
Уполномоченный сотрудник Банка

фамилия, инициалы подпись

		ч			м				
						2	0		

Приложение № 3 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

Системные требования

Для работы с системой «Электронный банк» необходимо:

1. Компьютер или ноутбук

- Браузер:
  - Microsoft Internet Explorer 11+
  - Mozilla Firefox 27+
  - Google Chrome 37+
  - Safari 5+
- Телефон подвижной сотовой радиотелефонной связи, находящийся в зоне доступа сети и способный получать СМС-сообщения;
- USB-порт.

2. Мобильное устройство:

- Операционная система:
  - IOS 7+
  - Android 4.3+
- Доступ в Internet:
  - 3G/4G
  - Wi-Fi
- Установленное бесплатное мобильное приложение «Электронный банк», доступное в магазинах Google Play и AppStore;
- Телефон подвижной сотовой радиотелефонной, находящийся в зоне доступа сети и способный получать СМС-сообщения.

3. Дополнительное оборудование:

- Принтер.

Приложение № 4 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

Уважаемый Клиент,

На основании п.7.2 «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» уведомляем Вас о том, что с «_ _ ___»_____20__ __г. Ваше дистанционное банковское обслуживание будет приостановлено в связи с неоплатой или неполной оплатой услуг Банка.

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ | _____

фамилия, инициалы | подпись

						2	0		

М.П.

Приложение № 5 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ О ПРЕКРАЩЕНИИ ПРЕДОСТАВЛЕНИЯ ДБО

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

На основании п.8.7. «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу Вас прекратить предоставление дистанционного банковского обслуживания моих банковских счетов на указанном ниже условии:

☐ - на период до ;

☐ - считать Договор о дистанционном банковском обслуживании расторгнутым.

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

М.П.

Приложение № 6 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ПРЕДОСТАВЛЕНИЯ ДБО

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

На основании п.5.6. «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу Вас снять блокировку с моей работы в системе «Электронный банк» и возобновить предоставление услуг ДБО.

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

Принято к исполнению
Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

		ч			м				
						2	0		

М.П.

Приложение № 7 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

На основании п.6.20 «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу Вас:

☐ - отменить ранее установленные ограничения

☐ - установить возможность доступа к Электронному банку со следующих IP адресов (хосты или подсети):

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

Клиент _____ _____
подпись фамилия, инициалы

__.__.20__

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

__.__.20__

М.П.

Приложение № 8 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ КЛИЕНТА

1. ФИО Клиента: _____
2. Адрес регистрации: _____ 3. ИНН _____
4. Паспорт: _____ серия _____ номер _____ дата выдачи «_____» _____ года кем выдан _____
5. Идентификатор ключа: _____
6. Наименование криптосредств: _____
7. Алгоритм: _____ ID набора параметров алгоритма: _____
8. Дата начала действия: «_____»_____20___г.
9. Дата окончания действия: «_____»_____20___г.
10. 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 проверки электронной подписи _____ (фамилия, инициалы) _____ (подпись)

						2	0		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ (фамилия, инициалы) _____ (подпись)

						2	0		

Приложение № 9 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ БАНКЕ

В целях обеспечения информационной безопасности при работе в Электронном банке **Клиент обязуется**:

1. Осуществлять вход в Электронный банк только через корпоративный сайт АО «МОСКОМБАНК», используя адрес https:\\mypay.moscombank.ru, либо через специальное приложение, которое может быть установлено на мобильное устройство из магазинов AppStore или GooglePlay.
2. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену москомбанк.рф, 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 подобных электронных писем, а также не рассылает по электронной почте программы для установки на компьютеры Клиентов. Связь с Клиентами поддерживается по телефону лично или средствами Электронного банка.
3. Не отлучаться от компьютера в период активной сессии с Электронным банком, особенно пока к нему подключен USB-токен или другой носитель, содержащий ключ ЭП.
4. Извлекать из компьютера USB-токен или другой носитель, содержащий ключ ЭП, сразу после завершения работы в Электронном банке.
5. Не передавать пароли, PIN-коды и коды доступа, USB- и OTP-токены или другие устройства, содержащие ключ ЭП, другим лицам, в том числе сотрудникам Банка для проверки работоспособности или настройки Электронного банка, хранить их в надежном месте, исключающем доступ к ним посторонних лиц. Вся ответственность за сохранность и использование ключей ЭП, одноразовых паролей, а также логина, пароля, PIN-кода для доступа к Электронному банку, полностью лежит на Клиенте, как единственном их владельце.
6. В случае выявления явных или косвенных признаков компрометации ключа ЭП, а также обнаружения вредоносных программ в компьютере, используемом для работы в Электронном банке, незамедлительно уведомить об этом Банк по телефону: (495) 609-19-19 доб.511, либо лично явиться в Банк с целью блокирования скомпрометированных данных с последующей их заменой. К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

- утеря USB- или OTP-токена или другого устройства, содержащего ключ ЭП, в том числе с последующим обнаружением;
- выход из строя USB- или OTP-токена или другого устройства, содержащего ключ ЭП, 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) идентификаторов учетной записи или одноразовых паролей доступа к Электронному банку неуполномоченных лиц (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Электронного банка, в том числе возникающих в связи с попытками нарушения информационной безопасности;

• обнаружение воздействия вредоносного кода в компьютере, используемом для работы в Электронном банке.

7. В случае выявления явных или косвенных признаков компрометации пароля учетной записи менять данный пароль самостоятельно.

8. Обеспечивать конфиденциальность использования паролей доступа, PIN-кодов, одноразовых паролей, которые не требуется сотрудникам Банка для обслуживания Клиента и поддержки Электронного банка в работоспособном состоянии.

9. Применять на компьютерах, используемых для работы Электронного банка, лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, антиспам-фильтры и т.п.

10. Производить периодическую (не реже 1 раза в 3 месяца) смену долговременного пароля и/или смену ключей ЭП, а также по требованию Банка и в случае компрометации. Не использовать простые пароли (123, qwerty, имена, даты рождения и т.д.).

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

12. Не использовать на своем компьютере 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).

13. 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.

14. Не заходить в Электронный банк через приложения для мобильных устройств на базе Android и iOS с того же мобильного устройства, на которое приходят СМС-сообщения с подтверждающим одноразовым паролем. Использовать в таких ситуациях OTP-токены для генерации одноразовых паролей.

15. Не устанавливать на мобильное устройство, используемое для приема СМС-сообщений с подтверждающим одноразовым паролем, приложения, полученные от неизвестных Вам источников. Помните, что Банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email сообщения.

16. При утрате мобильного устройства, используемого для приема СМС-сообщений с подтверждающим одноразовым паролем, немедленно обратиться к оператору сотовой связи и заблокировать SIM-карту. После этого связаться с Банком для временного прекращения предоставления доступа к Электронному банку и проверки последних платежей.

Помимо указанных выше требований **Банк рекомендует**:

1. Перед началом работы проверить наличие защищенного (шифрованного) соединения с сервером Электронного банка: символ замка и буква «S» в адресной строке – https://mypay.moscombank.ru, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.

2. Исключить доступ посторонних лиц к компьютеру, использующегося для работы в Электронном банке. Осуществлять постоянный контроль отправляемых платежных электронных документов при работе в Электронном банке, а также состояние своего личного счета.

3. Избегать работы в Электронном банке при подключении к публичным точкам доступа Wi-Fi, в интернет-кафе и на других компьютерах общего пользования, контролировать информацию об IP-адресе, с которого осуществлялся предыдущий вход в Электронный банк.

4. 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 лица.

5. 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.
6. В качестве дополнительной меры по обеспечению информационной безопасности воспользоваться предоставляемой Банком возможностью IP-фильтрации (разрешение доступа к Электронному банку только с указанных Клиентом IP-адресов/сетей).

Приложение № 10 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ ОБ ИЗМЕНЕНИИ НОМЕРА ТЕЛЕФОНА ДЛЯ СМС-СООБЩЕНИЙ

ФИО частного клиента – физического лица

Реквизиты документа, удостоверяющего личность

В соответствии с п.10.2. «Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу внести следующие изменения:

☐ - Зарегистрированный номер телефона для СМС-сообщений на + ( ) ;

в связи с

Подтверждаю, что данный телефонный номер, обслуживаемый оператором подвижной сотовой радиотелефонной связи, оформлен на мое имя и принадлежит мне на законных основаниях.

От Клиента _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

М.П.

Приложение № 11 к Правилам дистанционного обслуживания частных клиентов в системе Электронный банк

МОСКОМБАНК
Commercial Bank of Moscow

АКТ ПРИЕМА-ПЕРЕДАЧИ

Ф.И.О. частного клиента – физического лица

_____

_____

В соответствии с «Правилами дистанционного обслуживания частных клиентов в Электронном банке АО «МОСКОМБАНК» я получил(а):

☐ - ОТР-токен, аппаратное устройство позволяющие генерировать одноразовые пароли, идентификатор ОТР токена _____.

Комиссию за выдачу ОТР-токена, в соответствии с тарифами Банка прошу:

☐ - списать с моего счета у Вас № _____;

☐ - принять наличными в кассу Банка.

От Клиента _____ _____
подпись фамилия, инициалы

От Банка _____ _____
подпись фамилия, инициалы

						2	0		