

УТВЕРЖДЕНЫ
Правлением АО «МОСКОМБАНК»
Протокол № 01-05/36 от 30.10.2020
Введены в действие с 06.11.2020
Приказом № 01-08/73 от 02.11.2020



МОСКОМБАНК

Commercial Bank of Moscow

ПРАВИЛА
дистанционного обслуживания частных клиентов
в системе «Электронный банк»
АО «МОСКОМБАНК»
(версия 2.3)

Москва
2020

1. ОПРЕДЕЛЕНИЯ

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

Банк – АО «МОСКОМБАНК».

Клиент – физическое лицо, совершающее операции, не связанные с предпринимательской деятельностью или частной практикой.

Сторона – Банк или Клиент, совместно именуемые Стороны.

Счет – банковский счет (вклад), в том числе специальный карточный счет Клиента, открываемый на основании договора, заключенного между Банком и Клиентом.

Электронный банк (ЭБ) – электронное средство платежа, то есть способ, позволяющий Клиенту составлять, удостоверить и передавать в Банк распоряжения в целях осуществления перевода денежных средств, а также предоставления Клиенту информации о совершаемых/совершенных операциях с использованием информационно-коммуникационных технологий и/или электронных носителей информации, а физически – программа для ЭВМ - мобильное приложение или веб-решение, которое Банк предлагает Клиентам для доступа к предоставляемым банковским услугам. Поставщиком ЭБ является ООО «АйСимплЛаб» (ОГРН: 1127746023437, ИНН: 7704799375, место нахождения: г. Москва, ул. Большая Тульская, д. 10, стр. 9).

АБС – автоматизированная банковская система, обеспечивающая посредством ЭБ 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 ЭД, содержащих указание Клиента Банку о совершении соответствующей операции, составленное и переданное посредством ЭБ.

ЭД – электронный документ, то есть совокупность информации в цифровой форме, содержащая финансовый или иной документ, информационное или служебное сообщение в ЭБ.

Правила – настоящие Правила дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК».

Заявление – заявление на регистрацию в электронном банке (по форме Приложения № 1 к Правилам), направляемое Клиентом Банку.

Договор – заключенный между Банком и Клиентом договор дистанционного банковского обслуживания, включающий в себя Заявление, Правила, Тарифы, любые другие заявления Клиента, относящиеся к услугам, предоставляемым в рамках указанного Договора, а также иные документы в случаях, прямо оговоренных Сторонами.

Идентификаторы учетной записи Клиента – уникальная пара цифровой информации (логин и пароль), многократно используемая для аутентификации Клиента в ЭБ и однозначно выделяющая (идентифицирующая) Клиента среди определенного множества клиентов Банка.

Аутентификация – процедура проверки подлинности вводимых идентификаторов учетной записи путем сравнения введенного Пароля с хранящимся в базе данных Банка и сопоставления их введенному логину Клиента.

Пароль – общее название всех паролей Клиента, используемых при работе с ЭБ. К Паролям относятся: долговременный пароль учетной записи Клиента; пароль для доступа к секретному ключу ЭП; Одноразовый пароль, отправляемый в СМС или Пуш-сообщении; Одноразовый пароль, генерируемый OTP-токеном.

Одноразовый пароль – уникальный случайно образованный одноразовый набор символов, направляемый Клиенту на Авторизованный номер телефона в виде СМС или Пуш-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 обслуживании 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 (SMS) – сообщение, отправленное Банком через оператора подвижной сотовой радиотелефонной связи Клиенту на его Авторизованный номер телефона.

Пуш-сообщение (Push) – короткое сообщение, направляемое Банком в интернет-браузер Клиента на его устройство.

Авторизованный номер телефона – номер личного мобильного телефона Клиента, предоставленный (указанный) Клиентом Банку, единственным владельцем и пользователем которого является Клиент. Данный номер телефона является базовым идентификатором банковского счета Клиента в Банке в целях получения Клиентом услуг Банка с использованием ЭБ.

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 ЭП является электронной подписью, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Клиентом.

Усиленной неквалифицированной ЭП 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 ЭБ и предназначенный для создания Клиентом ЭП для ЭД.

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

Подлинная ЭП – 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 уполномоченного лица в том числе в соответствии с карточкой с образцами подписей и оттиска печати (в случае ее наличия в Банке).

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

СКЗИ – средства криптографической защиты информации (СКЗИ «КриптоПро CSP» (версия 4.0) компании ООО «КРИПТО-ПРО», входящее в состав ЭБ и АБС и имеющее сертификаты ФСБ России от 14.12.2018 № СФ/114-3567, 14.12.2018 № СФ/114-3568, 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.

ОТР-токен – аппаратное устройство, предназначенное для генерации Одноразовых паролей.

АСП – аналог собственноручной подписи – простая ЭП, которая посредством использования идентификационной пары (логина и пароля) и Одноразового пароля подтверждает факт формирования ЭП и используется для подтверждения авторства ЭД.

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 Распоряжения, 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 ЭП, 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 ЭД означает, что данный документ создан в ЭБ без отступлений от принятой технологии.

Целостность ЭД означает, что после его создания и заверения ЭП в его содержание не вносились никаких изменений.

Авторство ЭД – это свидетельство того, что ЭД создан и подписан пользователем ЭБ.

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 – ЭД, 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.

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

ЦЛСЗ ФСБ России – Центр по лицензированию, сертификации и защите государственной тайны ФСБ России.

СБП – Система быстрых платежей платежной системы Банка России.

Сайт – официальный сайт Банка в сети интернет: moscombank.pф (<https://moscombank.ru>).

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

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила определяют порядок предоставления Банком Клиентам дистанционного банковского обслуживания с помощью ЭБ, который позволяет получать дистанционный доступ к Счетам, передавать электронные расчетные документы, в том числе в СБП, принимать выписки по Счетам, передавать и принимать иные документы, информационные и сервисные сообщения, а также подключать и отключать Услуги.

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

2.3. Заключение Договора между Банком и Клиентом осуществляется путем присоединения Клиента к изложенным в Правилах условиям в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Направляя в Банк Заявление, Клиент заявляет о своем присоединении в полном объеме к Правилам. Договор считается заключенным между Сторонами с момента, указанного в пункте 11.1 Правил.

2.4. Доступ к ЭБ 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 Правилам ознакомился и проинформирован об условиях использования ЭБ, в частности о любых ограничениях способов и мест использования, случаях повышенного риска его использования как электронного средства платежа.

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

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

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

2.7.1. Информация, переданная Банком Клиенту с использованием ЭБ, считается доведенной до сведения Клиента по истечении 1 (Одного) дня с момента ее передачи Клиенту, независимо от фактического восприятия информации Клиентом (независимо от того, прочитана информация или нет).

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

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

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

2.10. Изменения/дополнения Правил считаются принятыми Клиентом, если Клиент с даты доведения до сведения Клиента указанной информации, определяемой согласно пункту 2.6 Правил, продолжает пользоваться ЭБ, в том числе, но не ограничиваясь, совершает операции, исполняет обязанности и осуществляет права по Договору, обращается в Банк, в том числе по телефону, с использованием интернета или по ЭБ по вопросам, связанным с использованием ЭБ и/или СБП, за исключением представления заявления о расторжении Договора.

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

2.12. Услуги по СБП, доступные в ЭБ, предоставляются на основании принятых в Банке «Правил осуществления переводов денежных средств в рамках системы быстрых платежей платежной системы Банка России».

2.13. ЭБ предоставляется Клиенту через вэб-интерфейс и/или специальное приложение, которое может быть установлено на мобильное устройство из интернет-магазинов AppStore или Play Market.

2.14. Взаимодействие ЭБ и АБС осуществляется с использованием информационно-телекоммуникационной сети интернет, к которой должно быть подключено устройство Клиента, на котором используется ЭБ.

2.15. Состав и содержание сервисов ЭБ, доступных Клиенту, определяется Банком и может меняться им по своему усмотрению и без предварительного уведомления.

3. ДОСТУП К ЭБ

3.1. Доступ к ЭБ предоставляется при наличии технической возможности круглосуточно в режиме 7/24 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 ЭБ с Сайта;

или

- перейти по интернет-ссылке <https://mypay.moscombank.ru>;

или

- воспользоваться мобильным приложением, установив его на свое мобильное устройство из магазинов AppStore или Play Market.

3.3. Для подтверждения доступа в ЭБ, направления в Банк Распоряжений, в иных случаях, установленных Банком, используются Одноразовые пароли, направляемые Клиенту в виде СМС-сообщения или Пуш-сообщения на его Авторизованный номер телефона, либо сгенерированные с помощью ОTR-токена Клиента.

3.4. Для подтверждения доступа в ЭБ через мобильные устройства может использоваться дополнительная идентификация Клиента посредством PIN-кода, который привязывается к конкретному мобильному устройству Клиента.

3.5. Регистрация Клиента автоматически прекращается, если с момента последнего доступа Клиента в ЭБ прошло более 2 (Двух) лет.

4. ДОКУМЕНТЫ

4.1. Стороны договорились использовать в электронной форме любые документы, предусмотренные законодательством Российской Федерации, нормативными актами Банка России и Банка (платежные поручения, распоряжения на перевод иностранной валюты, поручения на покупку/продажу/конвертацию иностранной валюты, выписки по Счетам), запросы, письма, уточнения, отзывы, уведомления, заявления на подключение или отключение банковских услуг, а также иные документы, не являющиеся платежными, составленные в свободном формате, в том числе документы валютного контроля (информация об ожидаемых сроках репатриации иностранной валюты и (или) валюты Российской Федерации, информация об осуществленной операции по договору займа и т.п.), иные документы Клиента и Банка.

4.2. По требованию Банка Клиент обязан в течение 2 (Двух) дней предоставить на бумажном носителе любой документ, указанный в пункте 4.1 Правил, подписав его собственноручной подписью.

4.3. Документы, указанные в пункте 4.1 Правил, изготавливаются в электронной форме на основе использования ЭБ. Форматы документов в электронной форме формируются ЭБ.

4.3.1. Если программное обеспечение ЭБ не предусматривает создание ЭД, то он может быть создан Клиентом с использованием иного программного обеспечения. В таком случае Электронный документ направляется в Банк в виде прикрепленного файла к письму.

4.5. Отображение ЭД на бумажном носителе осуществляется путем его распечатки на принтере исключительно через ЭБ.

4.6. Подлинником ЭД 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 программными средствами АБС, с использованием ключей проверки ЭП, зарегистрированных в установленном Правилами порядке. Результаты проверки подлинности фиксируются с использованием программных средств АБС.

4.7. Если ЭБ содержит в себе другой вложенный ЭД (например, письмо, созданное средствами ЭБ, содержит в себе прикрепленный сканированный документ Клиента), то АСП или ЭП Клиента, проставленная на первом ЭД, считается проставленной и на другой вложенный ЭД.

5. СОГЛАШЕНИЯ СТОРОН

5.1. Стороны признают, что:

5.1.1. Используемый в ЭБ механизм Аутентификации является достаточной мерой защиты от доступа третьих лиц к информации по Счетам Клиента.

5.1.2. Использование АСП или ЭП является достаточной мерой подтверждения Подлинности и Авторства ЭД.

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.

5.1.6. Клиент заявляет о признании Подлинности и надлежащего подписания АСП всех документов, направляемых Клиентом в Банк посредством сервиса ЭБ «Моя почта», включая вложенные ЭД в соответствии с пунктом 4.7 Правил. В этом случае в качестве АСП применяется сочетание логина, пароля и Одноразового пароля, которые использовал Клиент для входа в ЭБ.

5.2. В соответствии с положениями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» используемая в ЭБ ЭП на основе российских криптоалгоритмов признается Сторонами усиленной неквалифицированной ЭП, а используемые коды, пароли или иные средства (в том числе, направляемые посредством СМС-сообщений на Авторизованный номер телефона), подтверждающие факт формирования ЭП 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). При этом в целях предотвращения злонамеренного удаленного доступа к USB-токену рекомендуется вставлять его в компьютер только на время проставления ЭП, после чего извлекать.

5.3. Стороны признают, что при произвольном изменении ЭД, 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 ЭД 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 ЭД, 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. ЭД без ЭП или АСП Клиента не имеют юридической силы, Банком не рассматриваются и не исполняются.

5.6. Стороны признают, что ЭД с ЭП или АСП Клиента, создаваемые в АБС, являются доказательным материалом для решения спорных вопросов в соответствии с разделом 12 Правил. ЭД, 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 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 ЭБ в сети интернет согласно пункту 3.1 Правил в рабочие часы Банка, исключая технические перерывы, о которых сообщается отдельно.

6.2. ЭД, 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. ЭД, которые могут быть приняты, проверены, обработаны и исполнены без привлечения сотрудников Банка в автоматическом режиме, исполняются незамедлительно.

6.3. При получении ЭД Банк производит проверку подлинности ЭП или АСП Клиента, проверку правильности заполнения реквизитов ЭД, проверку на возможность возникновения дебето-

вого сальдо на Счете Клиента. Банк принимает к исполнению только ЭД, 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 ЭБ, разблокировав в АБС учетную запись Клиента, только при поступлении от Клиента соответствующего заявления (по форме Приложения № 6 к Правилам), заверенного собственноручной подписью Клиента.

6.6. Банк обязан хранить принятые от Клиента данные с АСП или ЭП в течение 5 (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 Правил, условий договора банковского счета, а также в иных аналогичных случаях Банк имеет право по своему усмотрению без уведомления Клиента блокировать доступ Клиента к ЭБ и не принимать к исполнению ЭД.

6.9. При наличии подозрений о компрометации учетной записи Клиента, ключа ЭП Клиента или неправильном их использовании Банк имеет право затребовать от Клиента оформленный в установленном порядке документ на бумажном носителе и не производить исполнения ЭД, сообщив об этом Клиенту не позднее следующего рабочего дня со дня получения соответствующего ЭД.

6.10. Банк имеет право на внесение изменений в программное обеспечение ЭБ 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 (Пятнадцать) календарных дней после уведомления Клиента в порядке, установленном пунктом 2.6 Правил.

6.12. Банк информирует Клиента о совершении каждой операции и/или обработке ЭД с использованием ЭБ путем направления Клиенту соответствующего уведомления одним или несколькими указанными ниже способами:

6.12.1. Путем изменения статуса его ЭД в режиме реального времени. Возможны следующие основные виды статусов в зависимости от типа ЭД:

- «Новый» - означает, что ЭД прошел контроль формата и для его отправки требуется ввести Одноразовый пароль из полученного СМС-сообщения или сгенерировать пароль при помощи OTP-токена;
- «В обработке» - означает, что ЭД прошел контроль формата и подтвержден при помощи СМС или Пуш-сообщения/OTP-токена, а также принят ЭБ в очередь на обработку и будет рассмотрен специалистом Банка в ближайшее время. Датой отправления ЭД в Банк является дата присвоения документу статуса «В обработке»;
- «Оплачен», «Завершен» - означает, что ЭД исполнен Банком, то есть Распоряжение отражено по Счету (проведено в балансе проводкой), иной документ принят и обработан Банком. Датой принятия ЭД является дата присвоения документу статуса «Оплачен» или «Завершен»;
- «Отказан» - означает отказ Банка в принятии ЭД. Датой непринятия Электронного документа является дата присвоения документу статуса «Отказан»;
- «Отменен» – означает отмену со стороны Клиента в принятии Банком на обработку данного ЭД. Использование Клиентом данного статуса возможно только до момента, пока направленному ЭД не присвоен статус «Оплачен» или «Завершен»;
- иные статусы, отражающие этапы обработки Электронного документа.

6.12.2. Путем предоставления Клиенту возможности получить в режиме реального времени информации об остатке денежных средств на Счете, а также о последних операциях по Счету посредством специально сформированного запроса в ЭБ.

6.12.3. Путем предоставления Клиенту возможности сформировать в режиме реального времени и распечатать выписку по Счету посредством специально сформированного запроса в ЭБ.

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) 109-00-14 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 3 (Трех) лет.

6.14. Для целей снижения риска хищения денежных средств Клиента в результате несанкционированного Клиентом доступа к ЭБ третьих лиц Банк имеет право устанавливать ограничения на сумму операции и/или совокупности операций за определенный период времени. При первом подключении Клиента к ЭБ ему устанавливаются ограничения, приведенные в Тарифах.

6.14.1. Клиент может изменить указанные ограничения в соответствии с пунктом 7.20 Правил.

7. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

7.1. На основании имеющихся у Банка лицензий ЦЛСЗ ФСБ России Клиент имеет право осуществлять эксплуатацию предоставленного Банком сертифицированного данным центром СКЗИ в ЭБ 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 ЭБ (Приложение № 3 к Правилам), а также то, что несанкционированное изменение конфигурации может привести к сбою в работе ЭБ.

7.3. Перед началом эксплуатации ЭБ и при использовании Усиленной неквалифицированной электронной подписи Клиент обязан 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 такой 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 представленное СКЗИ только в ЭБ, 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 ЭБ, включая представленное Банком СКЗИ.

7.6. Клиент не позднее следующего рабочего дня с момента обнаружения обязан сообщать Банку о возникновении следующих ситуаций:

- несанкционированного доступа или попытки такого доступа к ЭБ;
- совершения с помощью ЭБ платежа без согласия Клиента;
- потери (в том числе кратковременной) контроля над носителями секретного ключа ЭП или мобильного устройства, с которым связан Авторизованный номер телефона;
- компрометации ключей ЭП или логина и Пароля к ЭБ;
- отказа подтверждения программой проверки ЭП или АСП принимаемого или подписываемого в ЭБ;
- возникновения ошибки при совершении электронных платежей.

7.6.1. Под «ошибкой» понимается:

- 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 пункте 7.6 Правил 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 (по форме, установленной в Банке) одним из следующих способов:

- на бумажном носителе по факсу +7 (499) 242-82-19 с последующим предоставлением оригинала документа;
- на бумажном носителе в офис Банка по рабочим дням в рабочее время Банка. Адрес Банка указан на Сайте.

7.7. Клиент обязан в случае прекращения использования ЭБ удалить установленное на его компьютерах или мобильных устройствах программное обеспечение ЭБ, 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, с которым связан Авторизованный номер телефона, на который ЭБ 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 Клиента в Банке.

7.10. Клиент обязан обеспечить хранение ЭД в течение сроков, установленных законодательством Российской Федерации. Документы, подписанные ЭП, практическая необходимость в которых отпала и установленные сроки хранения которых истекли, могут быть уничтожены.

7.11. Клиент обязан сгенерировать новый ключ ЭП при Компрометации Пароля.

7.12. Клиент обязан обновлять программное обеспечение ЭБ и СКЗИ по требованию Банка или предложению электронных магазинов AppStore или Play Market.

7.13. Клиент имеет право досрочно прекратить действие своей учетной записи и/или своего активного ключа ЭП и потребовать от Банка заблокировать 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 сертификаты ключа проверки ЭП Клиента.

7.15. Клиент имеет право, позвонив по телефону в Банк, временно заблокировать свою работу в ЭБ. Такая устная блокировка должна сопровождаться предоставлением письменного уведомления (по форме Приложения № 5 к Правилам).

7.15.1. Такая блокировка возможна только при условии однозначной идентификации Клиента.

7.16. Клиент имеет право возобновить свою работу в ЭБ, которая ранее была заблокирована по его инициативе, представив в Банк Заявление на возобновление дистанционного банковского обслуживания в Электронном банке (по форме Приложения № 6 к Правилам).

7.17. Клиент имеет право представить в Банк Заявление на IP-фильтрацию (по форме Приложения № 7 к Правилам) и воспользоваться соответствующей услугой.

7.18. Клиент обязан внимательно ознакомиться и выполнять требования Инструкции по обеспечению информационной безопасности в Электронном банке (Приложение № 9 к 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 пункте 6.12 Правил.

7.20. Клиент имеет право изменить ограничения, которые устанавливает Банк для целей снижения риска хищения денежных средств Клиента путем несанкционированного доступа третьих лиц к счетам Клиента, лично подав в Банк заявление по форме Приложения № 12 к Правилам.

8. Размер и порядок оплаты услуг Банка

8.1. Клиент обязан оплачивать услуги Банка по предоставлению доступа к ЭБ, получению USB-токена и ОTR-токена в соответствии с Тарифами Банка.

8.2. В случае неоплаты или неполной оплаты услуг Банка в течение 2 (Двух) недель с момента, установленного Тарифами, Банк направляет Клиенту уведомление (по форме Приложения № 4 к Правилам) посредством ЭБ и прекращает предоставлять Клиенту услуг с использованием ЭБ.

8.3. Услуги, указанные в пункте 8.1 Правил, подлежат оплате путем списания Банком денежных средств с любого Счета Клиента, открытого в Банке, в порядке заранее данного акцепта. Присоединяясь к Правилам, Клиент заранее дает Банку акцепт при недостаточности денежных средств на Счете в валюте Российской Федерации/или при отсутствии Счета в валюте Российской Федерации списать денежные средства в погашение задолженности перед Банком с любо-

го Счета в иностранной валюте и поручает Банку произвести за счет Клиента конвертацию валюты, находящейся на Счете, по курсу и на условиях, установленных Банком для совершения конверсионных операций на дату такого списания.

9. ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. За неисполнение или ненадлежащее исполнение предусмотренных Правилами обязательств Стороны несут ответственность, предусмотренную законодательством Российской Федерации, за исключением возмещения упущенной выгоды.

9.2. При расторжении Договора Стороны несут ответственность по всем ЭД с ЭП и АСП, сформированным с помощью ЭБ, до момента такого расторжения.

9.3. Банк не несет ответственности за ущерб, причиненный 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 ЭБ в соответствии с пунктом 3.1 Правил, а для Клиента невозможность передачи Распоряжения 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 законодательства Российской Федерации.

9.6. В случае возникновения у Клиента технических неисправностей или других обстоятельств, препятствующих использованию ЭД, Клиент может обратиться в Банк с заявлением о прекращении предоставления ЭД на определенный срок или о расторжении Договора (по форме Приложения № 5 к Правилам).

9.7. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих исполнению ЭД, Банк вправе в одностороннем порядке отменить на неопределенный срок использование ЭД.

9.8. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием ЭБ, 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, пандемия, 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 В ЭБ

10.1. Использование Пароля

10.1.1. Клиент может самостоятельно изменять Пароль путем выполнения предусмотренной в ЭБ 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 ЭБ, без участия сотрудников Банка.

10.1.4. С целью повышения информационной безопасности при использовании ЭБ 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 ЭБ третьими лицами, Банк может устанавливать ограничения (лимиты) на сумму операции или совокупный объем операций за определенный период, совершаемых Клиентом с использованием ЭБ. Указанные ограничения устанавливаются Банком в зависимости от используемого Клиентом интерфейса (вэб-решение или приложение мобильного устройства).

10.2. Авторизованный номер телефона

10.2.1. В ходе самостоятельной регистрации в ЭБ, Клиент указывает Авторизованный номер телефона, который может использоваться ЭБ:

- как основной идентификатор Клиента в ЭБ;
- как основной идентификатор Клиента и получателя платежа в СБП;
- для получения СМС-сообщений с Одноразовыми паролями;
- для получения информации о совершаемой операции;
- для получения иной информации от Банка.

10.2.2. Клиент может изменить Авторизованный номер телефона путем представления в Банк письменного Заявления об изменении Авторизованного номера телефона, составленного по форме Приложения № 10 к Правилам.

10.2.3. Банк вправе без объяснения причин отказать Клиенту в регистрации в ЭБ и/или в изменении Авторизованного номера телефона.

10.2.4. Клиент обязуется исключить возможность использования иными лицами устройства, телефонный номер которого является Авторизованным номером телефона, 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 ЭБ. Доставка Одноразового пароля Клиенту может осуществляться следующими альтернативными методами:

- СМС-сообщением на Авторизованный номер телефона;
- Пуш-сообщения в веб-браузер Клиента на его устройстве;
- выводом пароля на экран ОTR-токена.

10.3.2. Срок действия Одноразового пароля, предоставленного Банком Клиенту, устанавливается Банком и указывается на экране ЭБ 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 ЭБ, 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-сообщения или Пуш-сообщения, содержащего Одноразовый пароль, произошедшее не по вине Банка.

10.3.7.1. Электронный банк информирует Клиента об отправке СМС-сообщения или Пуш-сообщения. Клиент имеет возможность активировать повторную отправку СМС-сообщения или Пуш-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 ЭБ.

10.4.2. Любая информация такого рода может быть предоставлена третьим лицам исключительно в порядке, установленном законодательством Российской Федерации.

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.

10.4.5. Основные правила Банка в области конфиденциальности установлены в Политике конфиденциальности в системе Электронный банк (Приложение № 13 к Правилам).

11. СРОК ДЕЙСТВИЯ ДОГОВОРА

11.1. Договор вступает в силу с момента получения Банком:

- Заявления в электронной форме, автоматически сформированного в процессе прохождения Клиентом в ЭБ процедуры регистрации;
- или Заявления на бумажном носителе по форме Приложения № 1 к Правилам.

11.2. Договор заключается на неопределенный срок.

11.3. Стороны вправе расторгнуть Договор. Договор считается расторгнутым с начала 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 возникновения спорных ситуаций между Клиентом и Банком при использовании ЭБ Стороны обязуются участвовать в рассмотрении споров в соответствии с разделом 13 Правил. При этом обмен ЭД между Сторонами прекращается.

12.3. Если Стороны не смогут урегулировать возникшие разногласия в претензионном порядке, спор передается в судебные инстанции города Москвы в зависимости от суммы требования, установленной законодательством: Мировому судье судебного участка № 366 района Хамовники города 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 города Москвы.

12.4. ЭД, 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 ЭБ операции (платежа), на которую Клиент не давал согласия.

13.2. В случае такого несогласия Клиент представляет Банку заявление о несогласии с операцией в соответствии с пунктом 7.6.2 Правил.

13.3. Заявление о несогласии с операцией рассматривается Банком в срок, не превышающий 30 календарных дней, а также в срок не более 60 календарных дней в случае осуществления Клиентом посредством ЭБ 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.

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, предусмотренной пунктом 6.12 Правил), в части выполнения Клиентом порядка направления в Банк заявления о несогласии с операцией и блокировки Ключа ЭП Клиента (пункт 7.6.2 Правил), а также законодательства Российской Федерации.

13.4.2. О мотивированном отказе в возмещении Клиенту суммы, указанной в заявлении о несогласии с операцией.

13.5. Банк в течение 5 (Пяти) рабочих дней с 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 ЭБ.

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 о прекращении действия учетной записи и/или электронного ключа (по форме Приложения № 2 к 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 ЭД 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 ЭД 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 ЭД 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 ЭП 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.



Приложение № 1
к Правилам дистанционного
обслуживания частных клиентов
в системе «Электронный банк»
АО «МОСКОМБАНК»

ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ В ЭЛЕКТРОННОМ БАНКЕ

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

Прошу АО «МОСКОМБАНК» (далее – Банк) предоставить доступ к системе дистанционного обслуживания «Электронный банк» в режиме просмотра информации о моих счетах, картах, вкладах, кредитах, иной информации 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.

В соответствии со статьей 428 Гражданского кодекса Российской Федерации уведомляю Банк о присоединении к Правилам дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» (далее – Правила). Подтверждаю, что ознакомлен, полностью согласен, присоединяюсь и обязуюсь исполнять указанные Правила и Тарифы Банка, являющиеся неотъемлемой частью Договора дистанционного банковского обслуживания (далее – Договор).

* 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» заключить Договор и 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»
АО «МОСКОМБАНК»



МОСКОМБАНК

Commercial Bank of Moscow

**УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ ДЕЙСТВИЯ УЧЕТНОЙ ЗАПИСИ
И/ИЛИ ЭЛЕКТРОННОГО КЛЮЧА**

Фамилия, имя, отчества (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании пункта 7.13 Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу Вас с _____ досрочно прекратить действие/блокировать:

- принадлежащую мне учетную запись в «Электронном банке» _____ ;

- ключ ЭП (ОТР-токен) со следующим идентификатором _____ .

Клиент _____ | _____
подпись фамилия, инициалы

						2	0		
--	--	--	--	--	--	---	---	--	--

Отметки АО «МОСКОМБАНК»

Принято к исполнению
Уполномоченный сотрудник Банка

_____ | _____
фамилия, инициалы подпись

		Ч							
						2	0		

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 Play Market 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»
АО «МОСКОМБАНК»



МОСКОМБАНК

Commercial Bank of Moscow

**УВЕДОМЛЕНИЕ О ПРЕКРАЩЕНИИ
ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
В СИСТЕМЕ ЭЛЕКТРОННЫЙ БАНК**

Уважаемый Клиент,

На основании пункта 8.2 Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» уведомляем Вас о том, что с «_» _____ 20__ г. дистанционное банковское обслуживание Ваших счетов будет приостановлено в связи с неоплатой/неполной оплатой услуг Банка.

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка

фамилия, инициалы

подпись

								2	0		
--	--	--	--	--	--	--	--	---	---	--	--

М.П.



МОСКОМБАНК

Commercial Bank of Moscow

**ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ
ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ В ЭЛЕКТРОННОМ БАНКЕ**

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании пункта 6.5 Правил дистанционного обслуживания частных клиентов в системе «Электронный банк» АО «МОСКОМБАНК» прошу Вас разблокировать учетную запись в системе «Электронный банк» и возобновить предоставление услуг дистанционного банковского обслуживания.

Клиент _____ | _____
подпись фамилия, инициалы

						2	0		
--	--	--	--	--	--	---	---	--	--

Отметки АО «МОСКОМБАНК»

Принято к исполнению
Уполномоченный сотрудник Банка

_____ | _____
фамилия, инициалы подпись

		ч				м			
						2	0		

М.П.



МОСКОМБАНК

Commercial Bank of Moscow

Приложение № 7
к Правилам дистанционного
обслуживания частных клиентов
в системе «Электронный банк»
АО «МОСКОМБАНК»

ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании 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

					2	0		
--	--	--	--	--	---	---	--	--

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____
фамилия, инициалы | подпись

					2	0		
--	--	--	--	--	---	---	--	--

М.П.



МОСКОМБАНК

Commercial Bank of Moscow

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ 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 Сайт, используя адрес <https://myraу.moscombank.ru>, либо через специальное приложение, которое может быть установлено на мобильное устройство из магазинов AppStore или Play Market.
2. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену moscombank.pф (<https://moscombank.ru>), сменить пароль доступа к нему, а немедленно сообщить о подобном факте в рабочие часы Банка по телефону (495) 109-00-14. 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) 109-00-14 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 файрволлы, анти-кейлоггеры, антиспам-фильтры.
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 (например, 123, qwerty, имена, даты рождения).
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 удаленного (дистанционного) доступа, которые обычно практикуют ИТ-специалисты для удаленной (дистанционной) поддержки (например, TeamViewer). 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 устанавливать на мобильное устройство, используемое для приема СМС или Пуш-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/e-mail сообщения.
15. При утрате мобильного устройства, используемого для приема СМС или Пуш-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://myraу.moscombank.ru>, в некоторых браузерах при защищенном соединении адресная строка будет подсвечена зеленым цветом.
2. Исключить доступ посторонних лиц к компьютеру, используемому 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 записывать используемый Пароль там, где доступ к нему могут получить посторонние лица.
5. Использовать только лицензионное, поддерживаемое производителем программное обеспечение (операционные системы, офисные пакеты), обеспечить автоматическое обновление системного и прикладного программного обеспечения, 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).



МОСКОМБАНК
Commercial Bank of Moscow

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ В СИСТЕМЕ ЭЛЕКТРОННЫЙ БАНК

Термины и определения

Банк – Акционерное общество «Московский Коммерческий Банк», сокращенное наименование – АО «МОСКОМБАНК».

Клиент – физическое лицо, заключившее с Банком договор на банковское обслуживание и являющееся пользователем ЭБ.

Обработка персональной информации (Обработка) – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональной информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональной информации.

Персональные данные – любые данные, относящиеся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Персональная информация – любая информация, которую Клиент в явной или неявной форме предоставляет о себе в процессе использования ЭБ, включая Персональные данные.

ЭБ – система Электронный банк программа для ЭВМ, Банка, позволяющая Пользователю получать банковское обслуживание (информационное и/или операционное) без посещения отделения обслуживания и непосредственного взаимодействия с сотрудниками Банка в рамках, заключенных договора банковского обслуживания и/или договора электронных денежных средств. К ЭБ относятся: веб-версия ЭБ для стационарных компьютеров, мобильные версии ЭБ для смартфонов и планшетов. Банк оказывает Клиенту услугу по предоставлению ЭБ только при наличии счета Клиента в Банке, открытого в соответствии с договором банковского счета.

Сайт – официальный сайт Банка в сети интернет: moscombank.рф (<https://moscombank.ru>).

Политика – настоящая Политика конфиденциальности в системе Электронный банк.

Главное

Настоящая Политика действует в отношении всей информации, которую Банк может получить о Клиенте во время использования им ЭБ.

Использование Клиентом ЭБ означает безоговорочное согласие Клиента с Политикой и указанными в ней условиями обработки его Персональной информации; в случае несогласия с этими условиями Клиент должен воздержаться от использования ЭБ.

Банк обеспечивает безопасность персональной информации, получаемой от Клиентов. Политика разработана с целью указания перечня данных, которые могут быть запрошены у Клиентов, а также способов обработки Банком и иными лицами таких данных. В Политике указаны цели,

для которых может запрашиваться или разглашаться Персональная информация Клиентов, а также указаны основные меры безопасности, которые должны предприниматься Клиентами для того, чтобы их персональная информация оставалась конфиденциальной.

Персональная информация

Клиенты передают Банку Персональные данные на основании заключаемых с Банком договоров. Порядок Обработки таких данных определяется соответствующими договорами. Персональная информация Клиентов, порядок Обработки которой не определен соответствующими договорами, обрабатывается в соответствии с данной Политикой.

Информация Клиентов собирается Банком в целях осуществления технического управления ЭБ, а также для проведения анализа и улучшения работы ЭБ; для предоставления Клиентам информации об оказываемых Банком услугах и предлагаемых Банком продуктах; в маркетинговых целях; в иных других целях, указанных в Политике или условиях использования ЭБ.

В ЭБ производится Обработка персональной информации следующих типов:

- информация, которую Клиент передает самостоятельно в процессе использования ЭБ, включая Персональные данные (например, при заполнении форм, заявок);
- информация, автоматически передаваемая в Банк в процессе использования ЭБ, в том числе IP-адреса, данные из cookies, информация об устройстве и браузере Клиента, времени активной сессии/подключения к системе и т.п. В общем случае Клиент не может контролировать передачу информации данного типа, ограничение передачи информации данного типа может нарушить функционирование ЭБ;
- информация о местоположении Клиента, автоматически передаваемая в Банк устройством Клиента. Клиент может контролировать передачу информации данного типа, изменяя настройки своего устройства.
- информация о совершаемых операциях. При совершении операций оплаты товаров и услуг, денежных переводов и прочего, Банком собираются данные о месте, времени и сумме совершенных операций, тип способа оплаты, данные о продавце и/или поставщике услуг, описания причины совершения операции, если таковые имеются, а также иную информацию, связанную с совершением указанных выше операций.

Банк не проверяет достоверность Персональной информации, предоставляемой Клиентами. Банк исходит из того, что Клиент предоставляет достоверную и достаточную Персональную информацию.

При использовании Персональной информации, а также иной информации, полученной Банком в процессе использования Клиентом функционала ЭБ, Банк руководствуется Политикой, внутриванковскими регламентами о защите персональных данных, а также законодательством Российской Федерации.

Цели сбора и обработки Персональной информации

Банк осуществляет Обработку только той Персональной информации, которая необходима для оказания услуг Клиенту.

Персональная информация может использоваться Банком в следующих целях:

- идентификация Клиента;
- предоставление Клиенту персонализированных сервисов;
- связь с Клиентом, в том числе направление уведомлений, запросов и информации, касающихся использования ЭБ, а также Обработка запросов, заявок и распоряжений Клиен-

- та;
- улучшение качества сервиса, удобства его использования, разработка новых услуг;
- проведение статистических и иных исследований на основе обезличенных данных, в том числе в целях создания рекламных материалов.

Сбор и использование информации, не являющейся персональной

Банк может осуществлять Обработку такой информации как уникальный идентификатор устройства, URL-адрес источника ссылки, часовой пояс, в котором находится Клиент. Целью такой обработки является изучение потребностей Клиента в целях предложения им наиболее подходящих продуктов, услуг. Банк может осуществлять Обработку сведений о действиях Клиентов при использовании ЭБ. Данная информация используется для оптимизации ЭБ.

При объединении информации, не являющейся Персональной, с Персональной информацией объединенная информация считается Персональной, пока она остается объединенной.

Сбор и использование информации, связанной с местоположением

Для предоставления сервисов, основанных на местоположении, Банк может собирать данные о географическом расположении компьютера или мобильного устройства Клиента, получаемые в режиме реального времени. Сервисы, основанные на местоположении, могут использовать данные GPS, ГЛОНАСС, Bluetooth, IP-адрес, а также другие технологии для определения точного или приблизительного местоположения компьютера или мобильного устройства. Данные о местоположении собираются анонимно в такой форме, которая не позволяет установить личность Клиента. Такие данные не являются Персональной информацией.

В ряде случаев Клиенту может быть предложено в явном виде определить свое местоположение. При объединении информации о местоположении Клиента с его Персональной информацией, объединенная информация считается Персональной, пока она остается объединенной. Данные о местоположении Клиентов используются Банком в целях предоставления и улучшения продуктов и услуг, использующих данные о местоположении.

Условия передачи Персональной информации третьим лицам

Банк вправе передать Персональную информацию третьим лицам в следующих случаях:

- Клиент выразил свое согласие на такие действия;
- передача необходима для исполнения распоряжения Клиента;
- если получение, использование и раскрытие такой информации необходимо с целью: выполнения и соблюдения законодательства, судебных решений или исполнение законных требований государственных органов; выявления, пресечения или иного воспрепятствования мошенничеству, а также устранения технических сбоев или проблем безопасности; защиты прав, собственности или безопасности Банка, Клиентов в рамках, допускаемых законодательством; когда у Банка имеются достаточные основания полагать, что Клиент нарушает условия Политики и заключенных с Банком договоров.

Для предоставления Банком информации Клиентов компаниям и частным лицам, не связанным с Банком, в том числе другим Клиентам, запрашивается дополнительное согласие Клиента, который в любое время может отозвать данное согласие.

Защита персональной информации Клиентов

Банк принимает необходимые и достаточные организационные и технические меры для защиты

Персональной информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц.

Банком постоянно совершенствуются способы Обработки данных, включая физические меры безопасности, для противодействия несанкционированному доступу к системам Банка с целью хищения имущества и иных видов мошенничества. Банком также ограничивается доступ сотрудников, подрядчиков и агентов к информации Клиентов, предусматривая строгие договорные обязательства в сфере конфиденциальности.

Безопасность использования ЭБ также зависит от соблюдения Клиентом рекомендаций, с которыми можно ознакомиться на Сайте. Клиент обязуется незамедлительно сообщать Банку о любом случае подозрения несанкционированного использования его учетной записи.

Изменение Политики

Банк имеет право в одностороннем порядке вносить изменения в Политику. Новая редакция Политики вступает в силу с момента ее размещения на Сайте.