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

МОСКОМБАНК
Commercial Bank of Moscow

ПРАВИЛА ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ЧАСТНЫХ КЛИЕНТОВ В АО «МОСКОМБАНК»

(версия 7.0)

Москва 2024

Оглавление

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В Правилах применяются термины и определения в соответствии со Стандартом Банка России СТО БР ИББС- 1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» и Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее - Федеральный закон № 63-ФЗ). 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.

Правила – настоящие Правила дистанционного обслуживания частных клиентов с использованием Интернет-банка и Мобильного приложения в АО «МОСКОМБАНК».
Банк – АО «МОСКОМБАНК».
Клиент – физическое лицо, совершающее операции, не связанные с предпринимательской деятельностью или частной практикой.
Сторона – Банк или Клиент, совместно именуемые Стороны.
Банковский счет (Счет) – банковский счет (вклад), в том числе специальный карточный счет Клиента, открываемый на основании договора, заключенного между Банком и Клиентом.
Банковская карта (Карта) - банковская карта, выпущенная Банком, расчеты по которой осуществляются за счет денежных средств Клиента, находящихся на Счете, предусматривающим совершение операций с использованием банковской карты.

Система ДБО – система дистанционного банковского обслуживания, позволяющая Клиенту составлять, удостоверять и передавать в Банк ЭД, в том числе, распоряжения в целях осуществления перевода денежных средств, а также предоставления Клиенту информации о совершаемых/совершенных операциях с использованием сети Интернет, представляющая из себя программу для ЭВМ, реализованную в виде - Интернет-банка и Мобильного банка. Разработчиком Системы ДБО является Закрытое акционерное общество «Центр финансовых технологий» (ИНН 5407125059, адрес 630055, Новосибирская область, Новосибирский район, рп Кольцово, д. 35), а разработчиком мобильных приложений – Закрытое акционерное общество «Центр цифровых сертификатов» (ИНН 5407187087, адрес 630055, Новосибирская область, г. Новосибирск, ул. Мусы Джалиля, д.11, каб. 309).
Интернет-банк - автоматизированная банковская система, обеспечивающая через информационно-телекоммуникационную сеть Интернет (далее - сеть Интернет) дистанционное банковское обслуживание (ДБО) Клиента посредством интернет-браузеров (веб-приложение) по адресу https://dbo.moscombank.ru.
Мобильный банк - автоматизированная банковская система, предоставляющая Клиенту возможность доступа к системе Интернет-банк, в виде мобильного приложения для установки на мобильное устройство на базе операционной системы iOS или Android.
АБС – автоматизированная банковская система, обеспечивающая посредством Системы ДБО 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 Системы ДБО.
ЭД – электронный документ, то есть совокупность информации в цифровой форме, содержащая финансовый или иной документ, информационное или служебное сообщение в Системе ДБО.
Заявление – заявление на регистрацию в Системе ДБО (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 Системе ДБО 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.

Логин – средство идентификации Клиента – код, используемый Клиентом при входе в Систему ДБО, и служащий для выделения Клиента среди других пользователей Системы ДБО.

Пароль – средство аутентификации Клиента, а также общее название всех паролей Клиента, используемых при работе с Системой ДБО. К Паролям относятся: долговременный пароль учетной записи Клиента и одноразовый пароль.

СМС-сообщение (SMS) – сообщение, отправленное Банком через оператора сотовой связи Клиенту на его Номер мобильного телефона.

Пуш-уведомление (Push) – короткое уведомление, направляемое Банком в мобильное приложение Клиента.

Номер мобильного 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 Системы ДБО.

Номер телефона Банка – номер телефона, который использует Банк для целей отправки СМС-сообщений, а также с которого могут осуществляться звонки Клиентам: +74951090014, +74956091919, +73833358811**;**

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) и его полномочий, подписывающего информацию. В Системе ДБО используется простая ЭП, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи Клиентом.

ПЭП ЕСИА - простая электронная подпись, полученная посредством обращения к Единой системе идентификации и аутентификации, которая подтверждает факт формирования электронной подписи конкретным лицом. При этом ключом ПЭП ЕСИА является сочетание 2-х элементов - Логина и Пароля.

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

Подлинность ЭД означает, что данный документ создан в Системе ДБО без отступлений от принятой технологии.

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

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

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.

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

СБП – Система быстрых платежей платежной системы Банка России.

ЕБС (Единая биометрическая система) - информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица - гражданина Российской Федерации.

ЕСИА (Единая система идентификации и аутентификации) - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, обеспечивающая в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Идентификация - определение сотрудником Банка личности Клиента по предъявленному Клиентом документу, удостоверяющему личность, или при использовании Средства аутентификации, а также определение Клиента Системой ДБО на основании Логина и Пароля, пин-кода, отпечатка пальца, иных кодов доступа, используемых при входе в Систему ДБО.

Удаленная идентификация - механизм, позволяющий Банку идентифицировать клиентов - физических лиц, без личного присутствия путем установления и подтверждения достоверности сведений о них, определенных Федеральным законом от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон №115-ФЗ), с использованием ЕСИА и ЕБС в порядке, установленном Федеральным законом от 27.06.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее - Федеральный закон №149-ФЗ), для предоставления таким клиентам финансовых услуг без посещения офиса Банка.

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

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

Претензия – заявление, направляемое Клиентом в Банк, в котором Клиент выражает несогласие с операцией, проведенной в Системе ДБО.

2. ЗАКЛЮЧЕНИЕ ДОГОВОРА

2.1. Настоящие Правила определяют порядок предоставления Банком Клиентам дистанционного банковского обслуживания с помощью Системы ДБО, который позволяет получать дистанционный доступ к Счетам и Картам, иной информации, 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 и сервисы Банка.

2.2. Договор может быть заключен в следующих случаях:

- с Клиентом, в отношении которого полностью завершены процедуры идентификации, и с которыми заключен договор банковского счета, открыт Счет или Карта;
- с Клиентом, не находящемся на обслуживании в Банке, в случае, если биометрические персональные данные Клиента размещены в ЕБС, при проведении Банком идентификации указанного Клиента путем установления и подтверждения достоверности сведений о нем с использованием ЕСИА и ЕБС в порядке, установленном Федеральным законом №149-ФЗ и Федеральным законом № 115-ФЗ.

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 любым из нижеперечисленных способов:

- путем личного обращения Клиента в офис Банка с направлением в Банк Заявления;
- дистанционно (для Клиентов, прошедших Идентификацию и находящихся в Банке на обслуживании) путем самостоятельного подключения услуги ДБО в Интернет-банке или с использованием Мобильного банка;
- с Клиентом, не находящемся на обслуживании в Банке, в случае, если биометрические персональные данные Клиента размещены в ЕБС, при проведении Банком идентификации указанного Клиента путем установления и подтверждения достоверности сведений о нем с использованием ЕСИА и ЕБС в порядке, установленном Федеральным законом №149-ФЗ и Федеральным законом № 115-ФЗ.

2.4. До заключения Договора Клиент обязан представить Банку достоверные сведения и информацию в соответствии с законодательством РФ и банковскими правилами, а в случае их изменения - предоставлять обновленные сведения и информацию в соответствии с договором банковского счета/договором банковского вклада.

2.4.1. Заключая Договор, Клиент дает свое согласие Банку на обновление информации о нем с использованием ЕСИА.

2.4.2. Заключая Договор, Клиент дает свое согласие Банку на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ "О персональных данных", полученных Банком с использованием ЕСИА.

2.4.3. Заключая Договор, Клиент дает свое согласие Банку на передачу персональных данных и сведений, составляющих банковскую тайну (в том числе, для обработки по поручению Банка), третьим лицам (операторам связи, интернет-провайдерам и др.), действующим на основании агентских договоров или иных договоров, заключенных ими с Банком с условием о конфиденциальности и неразглашении информации.

2.5. Для заключения Договора способом, перечисленным в п. 2.3 Правил, Клиент осуществляет следующие действия:

- в Интернет-банке или в Мобильном банке в специальном разделе вводит уникальные данные, позволяющие однозначно установить наличие его договорных отношений с Банком: фамилия, имя, отчество, а также сведения о номере Счета и/или номере Карты и/или реквизиты документа, удостоверяющего личность;
- самостоятельно создает Логин, используя разрешенные символы, и направляет в Банк запрос на получение временного Пароля. В ответ на полученный запрос Клиенту направляется временный Пароль, сформированный Банком, в виде СМС-сообщения на Номер мобильного телефона;

- для доступа в Систему ДБО Клиент вводит самостоятельно им сформированный Логин и полученный от Банка в виде СМС-сообщения временный Пароль. После ввода указанных данных Система ДБО предлагает Клиенту сформировать постоянный Пароль, который позволяет провести Аутентификацию Клиента в Системе ДБО.

2.5.1. Совершение Клиентом совокупности действий, указанных в настоящем пункте, признается согласием Клиента на присоединение к настоящим Правилам и заключение Договора. Договор считается заключенным с момента введения Клиентом Логина и временного Пароля.

2.5.2. Банк считает достаточным основанием полагать, что Договор заключен непосредственно с Клиентом, если лицом, обратившемся за получением услуги ДБО, были предоставлены в вышеуказанном порядке все необходимые сведения, а также введен временный Пароль, направленный в виде СМС-сообщения на Номер мобильного телефона Клиента. Риск убытков и иных неблагоприятных последствий вследствие доступа третьих лиц к сведениям, необходимым для самостоятельной регистрации в Системе ДБО, а также к Номеру мобильного телефона Клиента и/или Логину, Паролю, несет Клиент.

2.6. В случае заключения Договора с использованием ЕСИА Клиент осуществляет подписание Заявления ПЭП ЕСИА, полученной посредством обращения к ЕСИА.

2.6.1. Клиент в процессе прохождения Удаленной идентификации, также подписывает ПЭП ЕСИА согласие на обработку своих биометрических персональных данных.

2.6.2. При этом под биометрическими персональными данными Клиента понимаются сведения, которые характеризуют физиологические и биологические особенности Клиента, на основании которых можно установить его личность и которые используются Банком для установления личности субъекта персональных данных.

2.6.3. Под обработкой биометрических персональных данных, понимаются сбор и хранение, параметров биометрических персональных данных (данные изображения лица и данные голоса) в целях идентификации, осуществляемые с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №149-ФЗ. Согласие Клиента на обработку биометрических персональных данных действует со дня его подписания до дня его отзыва Клиентом путем личного обращения или направления письменного обращения (в том числе в форме электронного документа, подписанного простой электронной подписью или усиленной квалифицированной электронной подписью).

2.6.4. Необходимые для Удаленной идентификации сведения, предоставляются Клиентом Банку путем заполнения соответствующих форм, предоставления согласий, а также прохождением авторизации в ЕСИА.

2.6.5. Введением Логина и Пароля от своей учетной записи в ЕСИА (авторизацией) при заполнении форм в Интернет-банке или Мобильном банке признается согласием Клиента на присоединение к Правилам и заключение Договора, а также является заверением Клиента и гарантирует, что вся информация, размещенная в ЕСИА, и предоставляемая Банку в связи с заключением Договора, является верной, полной и точной. Банк руководствуется предоставленной в ЕСИА информацией при заключении Договора. При этом Банк вправе запросить иные дополнительные документы (сведения), необходимые для осуществления функций, возложенных на него действующим законодательством Российской Федерации и Центральным банком Российской Федерации (Банком России). Факт заключения Договора, после проведения Удаленной идентификации Клиента, подтверждается подключением Клиента к Системе ДБО.

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

2.8. 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 Системы ДБО;
- иными способами, позволяющими Клиенту получить информацию и установить, что она исходит от Банка.

2.9. 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.

2.9.1. Информация, переданная Банком Клиенту с использованием Системы ДБО, 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).

2.9.2. 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.

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

2.11. 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.

2.12. Изменения/дополнения Правил считаются принятыми Клиентом, если Клиент с даты доведения до сведения Клиента указанной информации, определяемой согласно пункту 2.8 Правил, продолжает пользоваться Системой ДБО, в том числе совершает операции, исполняет обязанности и осуществляет права по Договору, обращается в Банк, в том числе по телефону, с использованием Интернета или по Системе ДБО по вопросам, связанным с использованием Системы ДБО, за исключением представления заявления о расторжении Договора.

2.13. 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.

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

2.15. Система ДБО предоставляется Клиенту через веб-интерфейс в интернет-браузере (Интернет-банк) по адресу https://dbo.moscombank.ru и/или через мобильное приложение (Мобильный банк), которое может быть установлено на мобильное устройство Клиента из официальных интернет-магазинов (репозиториев) AppStore, Google Play или с официального сайта Банка.

2.16. Взаимодействие Системы ДБО и АБС осуществляется с использованием информационно-телекоммуникационной сети Интернет, к которой должно быть подключено устройство Клиента, на котором используется Система ДБО.

2.17. Состав и содержание сервисов Системы ДБО, доступных Клиенту, определяется Банком и может меняться им по своему усмотрению и без предварительного уведомления.

3. ДОСТУП К СИСТЕМЕ ДБО

3.1. Доступ к Системе ДБО предоставляется Клиенту после реализации им одного из способов заключения Договора, указанных в п. 2.3.
3.2. Доступ к Системе ДБО предоставляется при наличии технической возможности круглосуточно в режиме 24/7 с использованием сети Интернет, исключая технические перерывы, о которых сообщается отдельно. Техническая поддержка Клиентам предоставляется в рабочие часы Банка.
3.3. Для получения доступа Клиенту необходимо запустить Интернет-банк с Сайта или воспользоваться Мобильным банком на своем мобильном устройстве.
3.4. Средством идентификации Клиента при входе в Систему ДБО является Логин, а Средством аутентификации Клиента - Пароль. В процессе регистрации Клиента в Системе ДБО Клиенту присваивается временный Пароль, действующий при первом доступе в Систему ДБО и до момента изменения его Клиентом на постоянный Пароль. Временный пароль направляется Банком в виде СМС-сообщения на Номер мобильного телефона.
3.5. В случае превышения лимита попыток неверного ввода Клиентом Логина и/или Пароля при входе в Систему ДБО доступ в Систему ДБО автоматически блокируется. Возобновление доступа в Систему ДБО осуществляется любым нижеперечисленным способом:

- путем предоставления Клиентом письменного заявления на возобновление доступа к Системе ДБО в офисе Банка;
- путем самостоятельного возобновления доступа к Системе ДБО в Интернет-банке или в Мобильном банке.

3.6. Для подтверждения доступа в Систему ДБО, направления в Банк ЭД, в иных случаях, установленных Банком, используются одноразовые Пароли, направляемые Клиенту в виде СМС-сообщения или Пуш-уведомления.
3.7. Для подтверждения доступа в Мобильное приложение может использоваться дополнительная идентификация Клиента посредством пин-кода или отпечатка пальца, или биометрической информации об объемно-пространственной форме лица Клиента[1], который привязывается к конкретному мобильному устройству Клиента.
3.8. Регистрация Клиента автоматически прекращается, если с момента последнего доступа Клиента в Систему ДБО прошло более 2 (двух) лет.

[1] Функционал сканирования и проверки отпечатка пальца или биометрической информации об объемно-пространственной форме лица Клиента реализуется поставщиком мобильного устройства, например Face_ID, компании Apple.

4. ЭЛЕКТРОННЫЕ 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 и Картам), 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 Системы ДБО. Форматы документов в электронной форме формируются Системой ДБО.
4.3.1. Если программное обеспечение Системы ДБО не предусматривает создание ЭД, то он может быть создан Клиентом с использованием иного программного обеспечения. В таком случае ЭД направляется в Банк в виде прикрепленного файла к письму.
4.4. Отображение ЭД на бумажном носителе осуществляется путем его распечатки на принтере исключительно через Систему ДБО.
4.5. Подлинником ЭД является электронный образ документа в оговоренном формате, который содержит текст документа, 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.
4.6. Если Система ДБО содержит в себе другой вложенный ЭД (например, письмо, созданное средствами Системы ДБО, содержит в себе прикрепленный сканированный документ Клиента), то 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 Системе ДБО механизм Аутентификации является достаточной мерой защиты от доступа третьих лиц к информации по Счетам Клиента.
5.1.2. Использование ЭП является достаточной мерой подтверждения Подлинности и Авторства ЭД.
5.1.4. Использование IP-фильтрации является дополнительной мерой защиты при идентификации Клиента.
5.1.5. Риск неправомерного использования ЭП Клиента третьими лицами несет Клиент. Клиент заявляет о признании Подлинности и надлежащего подписания всех документов, заверенных ЭП, пока официально не будет объявлено о компрометации ЭП.
5.1.6. Клиент заявляет о признании подлинности и надлежащего подписания ЭП всех документов, направляемых Клиентом в Банк посредством Системы ДБО, включая вложенные ЭД в соответствие с пунктом 4.6 Правил.
5.2. Стороны признают, что при произвольном изменении ЭД, заверенного ЭП, целостность ЭД нарушается, то есть проверка ЭП дает отрицательный результат.
5.3. Стороны признают, что подделка ЭП Клиента, то есть создание Подлинной ЭП от имени Клиента, невозможна без знания идентификационных кодов, логина, паролей, позволяющих формировать ЭП определенным лицом.
5.4. Стороны признают, что ЭД, заверенные ЭП, юридически эквивалентны соответствующим документам на бумажном носителе, оформленным в установленном порядке (имеющим необходимые подписи и оттиск печати), обладают юридической силой и подтверждают наличие правовых отношений между Сторонами. ЭД без ЭП не имеют юридической силы, Банком не рассматриваются и не исполняются.
5.5. Стороны признают, что ЭД с ЭП, создаваемые в Системе ДБО, являются доказательным материалом для решения спорных вопросов в соответствии с разделом 9 Правил. ЭД, не имеющие ЭП, при наличии спорных вопросов, не являются доказательным материалом.
5.6. Стороны признают в качестве единой шкалы времени при работе с Системой ДБО московское поясное время. Контрольным является время системных часов АБС.
5.7. Стороны признают, что уведомления Банка, связанные с работой Системы ДБО, приостановлением доступа к Системе ДБО, приостановлением и отказом в исполнении ЭД, направляемые телефонограммой/СМС на телефон Клиента, доступный Банку и/или на электронную почту Клиента, и/или средствами Системы ДБО будут считаться надлежащим образом доставленными в день совершения уведомления Банком. Стороны каких-либо претензий друг к другу в связи с неполучением уведомления или с задержками в его получении иметь не будут.
5.8. Стороны признают, что действия Банка, связанные с приостановлением или отказом исполнения ЭД с признаками несанкционированных операций или с признаками рисковых операций не могут является основанием для предъявления требований о возмещении ущерба или упущенной выгоды.

6. ПРАВА И ОБЯЗАННОСТИ БАНКА

6.1. Банк обеспечивает гарантированную доступность Системы ДБО в сети Интернет согласно пункту 3.1 Правил круглосуточно, 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 Клиента, проверку правильности заполнения реквизитов ЭД, проверку на возможность возникновения дебетового сальдо на Счете или Карте. 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. Указанная блокировка производится в течение 30 минут с момента получения от Клиента соответствующего уведомления.
6.5. Банк обязан возобновить возможность работы Клиента в Системы ДБО, разблокировав в АБС учетную запись Клиента, только при поступлении от Клиента соответствующего заявления (по форме Приложения № 3 к Правилам), заверенного собственноручной подписью Клиента.
6.6. Банк обязан хранить принятые от Клиента данные с ЭП в течение 5 (пяти) лет.
6.7. При нарушении Клиентом порядка использования Системы ДБО в соответствии с Правилами и/или условий договора банковского счета Банк имеет право по своей инициативе приостановить или прекратить использование Клиентом Системы ДБО, в том числе ограничить функциональность Системы ДБО и не принимать к исполнению ЭД.
6.8. При наличии подозрений о компрометации учетной записи Клиента или неправильном их использовании Банк имеет право затребовать от Клиента оформленный в установленном порядке документ на бумажном носителе и приостановить исполнения ЭД.
6.9. Банк приостанавливает использование Клиентом Системы ДБО, если от Банка России и/или от федерального органа исполнительной власти в сфере внутренних дел получена информация, относящаяся к Клиенту и/или Системе ДБО, и/или иному средству платежа Клиента, о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.
6. 10. В случаях, указанных в п.п. 6.7 и - 6.8 Правил, Банк в день блокирования (приостановления или прекращения доступа Клиента к Системе ДБО) предоставляет Клиенту информацию о блокировании (приостановлении или прекращении) использования Системы ДБО с указанием причины такого блокирования (приостановления или прекращения).
6.11. В случае, указанном в п. 6.9 Банк в тот же день уведомляет Клиента о приостановлении использования Системы ДБО, а также о праве Клиента подать в порядке, установленном Банком России, в том числе через Банк, заявления об исключении сведений, относящихся к Клиенту, Системе ДБО, иному средству платежа Клиента, из базы данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента.
6.12. Указанная в 6.7 – 6.9 пунктах информация предоставляется Банком (вместе или по отдельности):

- телефонограммой с телефона Банка +7(495) 109-00-14 в рабочее время Банка;
- сообщением в Системе ДБО;
- объявлением при попытке авторизации Клиента в интерфейсе Системы ДБО;
- дополнительно СМС/Пуш-сообщением или сообщением электронной почты по реквизитам Клиента в автоматизированном и круглосуточном режиме (при наличии согласия Клиента).

6.13. Банк имеет право на внесение изменений в программное обеспечение Системы ДБО по собственному усмотрению и без предварительного уведомления.
6.14. Банк имеет право на внесение изменений в Правила в одностороннем порядке. Новая редакция Правил вступает в действие через 7 (семь) календарных дней после уведомления Клиента в порядке, установленном Правилами.
6.15. Для снижения риска хищения денежных средств Клиента в результате несанкционированного Клиентом доступа к Системе ДБО третьих лиц Банк имеет право устанавливать ограничения на сумму операции и/или совокупности операций за определенный период времени. При первом подключении Клиента к Системе ДБО ему устанавливаются ограничения, приведенные в Тарифах.

6.15.1. Клиент может изменить указанные ограничения в соответствии с пунктом 8.14 Правил.
6.16. Банк осуществляет в режиме реального времени анализ ЭД на предмет выявления ЭД с признаками несанкционированных операций или с признаками рисковых операций и предпринимать по собственному усмотрению действия, направленные на минимизацию последствий совершения несанкционированных операций или операций повышенного риска.
6.16.1. ЭД с признаками несанкционированных операций – это ЭД, соответствующий одному или нескольким признакам осуществления переводов денежных средств без добровольного согласия Клиента, установленным Банком России и размещенным на его официальном сайте в сети Интернет по адресу: https://cbr.ru/ с учетом требований Федерального закона «О национальной платежной системе» от 27/06/2011 № 161-ФЗ.
6.16.2. ЭД с признаками рисковых операций – это ЭД, соответствующий одному или нескольким признакам мошеннических операций, зафиксированным в аналитической системе Банка, за исключением признаков несанкционированных операций.
6.17. При выявлении ЭД с признаками несанкционированных или рисковых операций Банк имеет право приостановить или отказать в совершении операции, при этом Клиент информируется о:

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

6.17.1. Банк имеет право запросить у Клиента дополнительную информацию, подтверждающую, что исполнение ЭД не связано с переводом денежных средств без добровольного согласия Клиента.
6.17.2. Указанное в п. 6.17 информирование осуществляется Банком в порядке, аналогичном, изложенному в п. 6.12.
6.17.3. При непоступлении от Клиента подтверждения ЭД или повторного совершения ЭД в срок, установленый в п. 6.17, ЭД считается непринятым к исполнению, а повторная операция несовершенной.
6.17.4. При поступлении от Клиента в срок, указанный в 6.17, подтверждения ЭД или повторного ЭД, Банк исполняет распоряжение Клиента, кроме случая, указанного в 6.18.
6.17.4.1. В случае, если Клиент направляет подтверждение ЭД средствами ДБО в нерабочее время Банка, но с соблюдением срока, указанного в п. 6.17, обработка такого подтверждения производится Банком в первый рабочий день, следующий за днем этого подтверждения.
6.18. Если, несмотря на направление Клиентом подтверждения ЭД или осуществление действий по совершению повторной операции с ЭД, от Банка России получена информация, относящаяся к Клиенту и/или Системе ДБО, и/или иному средству платежа Клиента, о случаях и попытках осуществления переводов денежных средств без добровольного согласия Клиента, Банк приостанавливает исполнение подтвержденного ЭД на два дня со дня направления Клиентом подтверждения или отказывает в совершении повторной операции. При этом применяется оговорка п. 6.17.4.1 о нерабочем дне Банка.
6.18.1. Банк в порядке, установленном п. 6.17 Правил, информирует Клиента о данном факте.
6.18.2. По истечении двух дней со дня направления Клиентом подтверждения ЭД, Банк незамедлительно принимает к исполнению подтвержденный ЭД (при отсутствии иных оснований не принимать ЭД к исполнению). При этом применяется оговорка п. 6.17.4.1 о нерабочем дне Банка.

6.18.3. По истечении двух дней со дня совершения Клиентом по совершению повторной операции Банк принимает к исполнению соответствующий ЭД.

7. ИНФОРМИРОВАНИЕ КЛИЕНТА О СОВЕРШЕННЫХ ОПЕРАЦИЯХ

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

7.1.1. Путем изменения статуса его ЭД в режиме реального времени. Возможны следующие основные виды статусов «Доставлен в Банк», «Исполнен», «Возвращен», «Отклонен» и другие. Клиент согласен с тем, что присвоение статуса «Исполнен» в Системе ДБО является надлежащим уведомлением Банком Клиента о совершении Банком соответствующей Операции по Счету.

7.1.2. Путем предоставления Клиенту возможности получить в режиме реального времени информации об остатке денежных средств на Счете или Карте, а также о последних операциях по Счету или Карте.

7.1.3. Путем предоставления Клиенту возможности сформировать в режиме реального времени выписку по Счету, выбранного формата, посредством специально сформированного запроса в Системе ДБО[2].

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

7.1.5. 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 или Карте и последних операциях, при условии однозначной идентификации Клиента.

7.2. Уведомление об операциях, совершенных по Счету или Карте с использованием Системы ДБО, способом, указанным в п. п. 7.1 Правил, осуществляется без взимания Банком комиссионного вознаграждения.

7.3. Уведомление о совершенной операции с использованием Системы ДБО считается полученным Клиентом в момент доступа Клиента к Системе ДБО, зафиксированного программным обеспечением Банка.

7.4. Банк фиксирует направляемые Клиенту уведомления и хранит их в течение 3 (трех) лет.

[2] Доступно только в Интернет-банке

8. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

8.1. Клиент обязан обеспечивать сохранность, безопасность и целостность программного комплекса Системы ДБО, а в случае прекращения использования удалить установленное, на его компьютерах или мобильных устройствах, программное обеспечение.
8.2. Клиент не позднее следующего рабочего дня с момента обнаружения обязан сообщать Банку о возникновении следующих ситуаций:

- несанкционированного доступа или попытки такого доступа к Системе ДБО;
- совершения с помощью Системы ДБО платежа без согласия Клиента;
- потери (в том числе кратковременной) контроля над техническим средством (мобильный телефон, ноутбук, компьютер, планшет и т.п.), с которым связан Номер мобильного телефона;
- компрометации Логина и Пароля к Системе ДБО;
- отказа подтверждения программой проверки ЭП принимаемого или подписываемого в Системе ДБО;
- возникновения ошибки при совершении электронных платежей.
- неприхода СМС-сообщений или Пуш-уведомлений;
- некорректном одноразовом Пароле (коде) в СМС-сообщении или в Пуш-уведомлении.

8.2.1. 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.

8.2.2. Указанное в пункте 8.2 Правил сообщение Банку будет считаться надлежащим образом направленным, если Клиент осуществит следующие действия:

- незамедлительно блокирует Систему ДБО 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 или электронной почте bank@moscombank.ru с последующим предоставлением оригинала документа;
    - на бумажном носителе в офис Банка по рабочим дням в рабочее время Банка. Адрес Банка указан на Сайте.

8.3. Клиент обязан хранить в секрете и не передавать третьим лицам Логин, Пароль и одноразовые Пароли (коды) СМС-сообщений и Пуш-уведомлений.
8.4. Клиент обязан ограничить доступ третьих лиц к своему устройству, с которым связан Номер мобильного телефона, на который Система ДБО направляет одноразовые Пароли.
8.5. 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.
8.6. Клиент обязан сгенерировать новый Пароль при Компрометации Пароля.
8.7. Клиент обязан обновлять программное обеспечение Системы ДБО по требованию Банка с Сайта или по предложению официальных интернет-магазинов (репозиториев) AppStore или Google Play .
8.8. Клиент имеет право досрочно прекратить действие своей учетной записи и потребовать от Банка блокировать свою учетную запись, оформив уведомление по форме Приложения № 2 к Правилам.

8.9. Клиент имеет право, позвонив по телефону +7 (495) 109-00-14 в Банк, временно блокировать свою работу в Системе ДБО. Такая устная блокировка должна сопровождаться предоставлением письменного уведомления (по форме Приложения № 2 к Правилам).
8.9.1. Такая блокировка возможна только при условии однозначной идентификации Клиента.
8.10. Клиент имеет право возобновить свою работу в Системе ДБО, которая ранее была заблокирована по его инициативе, представив в Банк Заявление на возобновление дистанционного банковского обслуживания (по форме Приложения № 5 к Правилам).
8.11. Клиент имеет право представить в Банк Заявление на IP-фильтрацию (по форме Приложения № 3 к Правилам) и воспользоваться соответствующей услугой.
8.12. Клиент обязан внимательно ознакомиться и выполнять требования Инструкции по обеспечению информационной безопасности в Системе ДБО (Приложение № 4 к Правилам).
8.13. 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 разделе 7 Правил.
8.14. Клиент имеет право изменить ограничения, которые устанавливает Банк для снижения риска хищения денежных средств Клиента путем несанкционированного доступа третьих лиц к счетам Клиента, лично подав в Банк заявление по форме Приложения № 7 к Правилам.
8.15. Клиент обязуется обеспечить наличие в Банке контактной информации о Номере мобильного телефона, необходимой для направления уведомлений о совершении операций использованием Системы ДБО способами, указанными в разделе 7 Правил, и поддерживать их в актуальном состоянии, если указанный способ уведомления выбран Клиентом.
8.16. В случае изменения Номера мобильного телефона, предоставленного в Банк для получения Клиентом уведомлений об Операциях, совершенных по Счету или Карте с использованием Системы ДБО, Клиент обязан своевременно представить в Банк измененную информацию.
8.16.1. Изменение информации о Номере мобильного телефона производится путем подачи в Банк письменного заявления на бумажном носителе в офис Банка и/или в электронном виде по Системе ДБО.
8.16.2. До момента предоставления Клиентом в Банк изменений контактной информации способом, указанным в настоящем пункте, Клиент принимает на себя риски, связанные с непредставлением Банку информации об изменении номера мобильного телефона и/или адреса электронной почты.
8.17. Клиент самостоятельно и за свой счет обеспечивает и оплачивает технические, программные и коммуникационные ресурсы, необходимые для организации получения направляемых Банком уведомлений о совершении Операций с использованием Системы ДБО.

9. ПРЕДЪЯВЛЕНИЕ ПРЕТЕНЗИЙ И ИХ РАССМОТРЕНИЕ

9.1. В случае несогласия со списанием со Счета или Карты какой-либо суммы денежных средств Клиент обязан направить в Банк Претензию в течение 10 (десяти) рабочих дней со дня совершения спорной операции, приложив к ней документы, подтверждающие совершение операции списания оспариваемой суммы денежных средств. При отсутствии обращения Клиента в Банк в срок, указанный в настоящем пункте, операция, совершенная по Счету или Карте с использованием Системы ДБО, считается подтвержденной Клиентом.
9.2. Банк рассматривает Претензию и предоставляет ответ Клиенту в течение 30 (тридцати) календарных дней со дня получения Претензии, а также не более 60 (шестидесяти) календарных дней со дня получения Претензии в случае осуществления трансграничного перевода денежных средств.
9.3. Банк вправе запросить у Клиента предоставление дополнительных документов и информации, необходимой для всестороннего рассмотрения Претензии, в том числе документы, подтверждающие обращение Клиента в правоохранительные органы Российской Федерации.
9.3.1. Клиент обязан по запросу Банка представить документы, которые необходимы Банку для всестороннего рассмотрения Претензии.
9.3.2. В случае непредоставления в Банк необходимых документов в течение 7 (семи) календарных дней с момента запроса Банком у Клиента недостающих документов Банк составляет мотивированный ответ о невозможности опротестования операции из-за недостаточности предоставленных Клиентом документов путем направления письменного уведомления Клиенту.
9.4. Если в ходе рассмотрения Претензии Клиента у Банка по объективным причинам возникают сложности в расследовании обстоятельств, в том числе связанные с запросом Банком необходимых документов, то срок её рассмотрения может быть увеличен, но не более чем на 30 (тридцать) календарных дней.
9.5. По результатам расследования Банк принимает решение о возмещении/отказе в возмещении оспариваемой суммы операции, совершенной по Счету или Карте с использованием Системы ДБО.
9.6. В случае принятия Банком решения о возмещении Клиенту оспариваемой суммы, Банк перечисляет оспариваемую сумму операции на Счет или Карту Клиента в течение 3 (трех) рабочих дней с даты принятия такого решения. В случае принятия Банком решения об отказе в возмещении суммы операции Банк направляет Клиенту письменное уведомление с обоснованием отказа ему в возмещении денежных средств по спорной операции.
9.7. 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.

10. РАЗМЕР И ПОРЯДОК ОПЛАТЫ УСЛУГ БАНКА

10.1. Клиент обязан оплачивать услуги Банка по предоставлению доступа к Системе ДБО в соответствие с Тарифами Банка.
10.2. В случае неоплаты или неполной оплаты услуг Банка в течение 2 (двух) недель с момента, установленного Тарифами, Банк направляет Клиенту уведомление посредством Системы ДБО и прекращает предоставлять Клиенту услуг с использованием Системы ДБО.
10.3. Услуги, указанные в пункте 10.1 Правил, подлежат оплате путем списания Банком денежных средств с любого Счета или Карты Клиента, открытого в Банке, в порядке заранее данного акцепта. Присоединяясь к Правилам, Клиент заранее дает Банку акцепт при недостаточности денежных средств на Счете или Карте в валюте Российской Федерации/или при отсутствии Счета или Карты в валюте Российской Федерации списать денежные средства в погашение задолженности перед Банком с любого Счета или Карты в иностранной валюте и поручает Банку произвести за счет Клиента конвертацию валюты, находящейся на Счете или Карте, по курсу и на условиях, установленных Банком для совершения конверсионных операций на дату такого списания.

11. ОБЯЗАТЕЛЬСТВА И ОТВЕТСТВЕННОСТЬ СТОРОН

11.1. За неисполнение или ненадлежащее исполнение предусмотренных Правилами обязательств Стороны несут ответственность, предусмотренную законодательством Российской Федерации, за исключением возмещения упущенной выгоды.
11.2. При расторжении Договора Стороны несут ответственность по всем ЭД с ЭП, сформированным с помощью Системы ДБО, до момента такого расторжения.
11.3. Банк не несет ответственности за ущерб, причиненный Клиенту в результате использования третьими лицами учетной записи Клиента, ЭП, одноразовых Паролей.
11.4. Банк не несет ответственности за сбои в работе линий связи и провайдеров, технических средств, программного обеспечения, повлекшие для Банка невозможность предоставления доступа к Системе ДБО, отправки СМС-сообщений, Пуш-уведомлений, а для Клиента невозможность передачи ЭД в электронной форме или получения информации о совершенных операциях.
11.5. Клиент несет риск убытков, которые могут возникнуть у него в результате несанкционированного использования его программно-технических средств, учетной записи, ЭП, одноразового Пароля, с учетом законодательства Российской Федерации.
11.6. 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 № 2 к Правилам).
11.7. В случае возникновения у Банка технических неисправностей или других обстоятельств, препятствующих исполнению ЭД, Банк вправе в одностороннем порядке отменить на неопределенный срок использование ЭД.
11.8. Стороны обязуются при разрешении экономических и иных споров, которые могут возникнуть в связи с использованием Системы ДБО, предоставлять в письменном виде свои оценки, доказательства и выводы.
11.9. 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.

12. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ РАБОТЫ В СИСТЕМЕ ДБО

12.1. Использование Пароля

12.1.1. Клиент может самостоятельно изменять Пароль путем выполнения предусмотренной в Системе ДБО процедуры смены Пароля.

12.1.2. Клиент обязуется обеспечить хранение информации о Пароле способом, делающим Пароль недоступным третьим лицам, а также немедленно уведомлять Банк о Компрометации Пароля.

12.1.3. Клиент не должен сообщать Пароль, иным лицам, сотрудникам Банка по телефону, электронной почте или иным способом. Использование Пароля допускается только при работе Клиента непосредственно в Системе ДБО, без участия сотрудников Банка.

12.1.4. С целью повышения информационной безопасности при использовании Системы ДБО с мобильных устройств для входа в систему может использоваться пин-код, отпечаток пальца, биометрические данные лица, которые привязываются к конкретному мобильному устройству Клиента.

12.1.5. С целью минимизации риска Клиента, связанного с несанкционированным использованием Системы ДБО третьими лицами и противодействия осуществлению переводов денежных средств без согласия Клиента, Банк и/или Клиент могут устанавливать:

- ограничения (лимиты) на сумму операции и/или совокупный объем операций за определенный период, совершаемых Клиентом с использованием Системы ДБО;
- IP-фильтрацию, т.е. запрет входа в Систему ДБО с каких-либо Интернет-адресов (IP-адресов), кроме указанных Клиентом.

12.1.5.1. Банк устанавливает, указанные выше ограничения и IP-фильтрацию в течение трех банковских дней с момента получения Банком соответствующего заявления Клиента.

12.2. Номер мобильного телефона

12.2.1. В ходе самостоятельной регистрации в Системе ДБО, Клиент указывает Номер мобильного телефона, который будет использоваться Системой ДБО как:

- основной идентификатор Клиента в Системе ДБО;
- основной идентификатор Клиента и получателя платежа в СБП;
- получения СМС-сообщений/Пуш-уведомлений с одноразовыми Паролями;
- для получения иной информации от Банка.

12.2.2. Клиент может изменить Номер мобильного телефона путем представления в Банк письменного Заявления об изменении Номера мобильного телефона, составленного по форме Приложения № 6 к Правилам.

12.2.3. Банк вправе без объяснения причин отказать Клиенту в регистрации в Системе ДБО и/или в изменении Номера мобильного телефона.

12.2.4. Клиент обязуется исключить возможность использования иными лицами устройства, телефонный номер которого является Номером мобильного телефона, а также немедленно уведомлять Банк об утрате или возникновении риска несанкционированного использования такого устройства.

12.3. Использование одноразовых Паролей

12.3.1. Подтверждение действий Клиента в Системе ДБО, применение ЭП 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 Системы ДБО. Доставка одноразового Пароля Клиенту может осуществляться следующими альтернативными методами:

- СМС-сообщением на Номер мобильного телефона;
- Пуш-уведомление в Мобильное приложение Клиента на его устройстве.

12.3.2. Срок действия одноразового Пароля, предоставленного Банком Клиенту, устанавливается Банком и указывается на экране Системы ДБО при его генерации.

12.3.3. Положительный результат проверки одноразового Пароля означает, что ЭП Клиента принята.
12.3.4. Клиент обязуется обеспечить хранение одноразовых Паролей способом, делающим их недоступными третьим лицам.
12.3.5. Клиент не должен сообщать одноразовые Пароли иным лицам, сотрудникам Банка по телефону, электронной почте или иным способом. Использование одноразовых Паролей допускается только при работе Клиента непосредственно в Системе ДБО, без участия сотрудников Банка.
12.3.6. Банк не несет ответственности за ущерб, возникший вследствие несанкционированного использования третьими лицами одноразовых Паролей.
12.3.7. Банк не несет ответственности за неполучение Клиентом СМС-сообщения или Пуш-уведомления, содержащего одноразовый Пароль, произошедшее не по вине Банка.
12.3.7.1. Система ДБО информирует Клиента об отправке СМС-сообщения или Пуш-сообщения. Клиент имеет возможность активировать повторную отправку СМС-сообщения или Пуш-уведомления в необходимых случаях.
12.3.8. 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.

12.4. Конфиденциальность

12.4.1. Банк обязуется принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Системы ДБО, храня и передавая ее в защищенном виде с использованием защищенных каналов связи, с использованием сети Интернет и локальных вычислительных сетей.
12.4.2. Любая информация такого рода может быть предоставлена, по запросу, третьим лицам исключительно в порядке, установленном законодательством Российской Федерации, а также при привлечении Банком третьих лиц к оказанию услуг в рамках ДБО
12.4.3. Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации по сети Интернет, в незащищенном виде с использованием незащищённых каналов связи, влечет риск несанкционированного доступа к такой информации третьих лиц.
12.4.4. 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.
12.4.5. Основные правила Банка в области конфиденциальности установлены в Политике конфиденциальности в Системе ДБО (Приложение № 8 к Правилам).

13. СРОК ДЕЙСТВИЯ ДОГОВОРА

13.1. Договор вступает в силу с момента получения Банком:

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

13.2. Договор заключается на неопределенный срок.

13.3. Стороны вправе расторгнуть Договор. Договор считается расторгнутым с начала рабочего дня, следующего за днем направления уведомления о расторжении Договора.

13.4. Договор считается автоматически расторгнутым, если с момента последней Аутентификации Клиента в Системе ДБО прошло более двух лет.

ПРИЛОЖЕНИЕ № 1 Заявление на регистрацию в Системе ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ В СИСТЕМЕ ДБО

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

Номер мобильного телефона

Прошу АО «МОСКОМБАНК» (далее – Банк) предоставить доступ к Системе ДБО в соответствии с Правилами.
В соответствии со статьей 428 Гражданского кодекса Российской Федерации уведомляю Банк о присоединении к Правилам дистанционного банковского обслуживания частных клиентов (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). Подтверждаю, что ознакомлен и полностью согласен с Политикой конфиденциальности в Системе ДБО в АО «МОСКОМБАНК». Подтверждаю, что ознакомлен и полностью согласен с Политикой защиты персональных данных в АО «МОСКОМБАНК».

С целью противодействия осуществления переводов денежных средств без моего согласия прошу Банк, с учетом Тарифов:

☐ - установить следующие ограничения в Системе ДБО, рублей*:

- все переводы в сутки: (по умолчанию 500 000);
- переводы по СБП в месяц: ** (по умолчанию не установлено);
- другие виды переводов _____ в сутки: .

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

№ п/п	IP-адрес/маска	№ п/п	IP-адрес/маска
1		3	
2		4	

* для валютных счетов будет применяться ограничение, рассчитанное по курсу Банка России на день совершения операции;
** - данное ограничение может быть установлено только клиентам, признанным несостоятельными (банкротами).

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

В соответствии с Правилами дистанционного банковского обслуживания частных клиентов в АО «МОСКОМБАНК» заключить Договор и подключить Клиента к Системе ДБО.

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

ПРИЛОЖЕНИЕ № 2 Заявление о прекращении/приостановлении ДБО или учетной записи

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ ОПРЕКРАЩЕНИИ/ПРИОСТАНОВЛЕНИИ ДБО ИЛИ ДЕЙСТВИЯ УЧЕТНОЙ ЗАПИСИ

Фамилия, имя, отчества (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании Правил дистанционного банковского обслуживания частных клиентов в АО «МОСКОМБАНК» прошу Вас:

☐ - приостановить дистанционное банковское обслуживание моих счетов на период до ;

☐ - с блокировать, принадлежащую мне учетную запись в Системе ДБО ;

☐ - считать Договор дистанционного банковского обслуживания расторгнутым.

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

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

		ч			м				
						2	0		

ПРИЛОЖЕНИЕ № 3 Заявление на IP-фильтрацию

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА IP-ФИЛЬТРАЦИЮ

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании Правил дистанционного банковского обслуживания частных клиентов в АО «МОСКОМБАНК» прошу Вас:

☐ - отменить ранее установленные ограничения

☐ - установить возможность доступа к Системе ДБО 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.

ПРИЛОЖЕНИЕ № 4 Рекомендации по снижению рисков перевода денежных средств без добровольного согласия клиента

МОСКОМБАНК
Commercial Bank of Moscow

РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ РИСКОВ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТА В СИСТЕМЕ ДБО

В области информационной безопасности АО «МОСКОМБАНК» рекомендует Клиенту:

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

2. Осуществлять вход в Систему ДБО только через Сайт https://dbo.moscombank.ru (Интернет-банк), либо через мобильное приложение (Мобильный банк), которое может быть установлено на мобильное устройство из рекомендуемых Банком интернет-магазинов (репозиториев), таких как AppStore, Google Play, RuStore и другие, или путем загрузки и установки аналогичного официального приложения с официального Сайта Банка.

3. Не отвечать на письма, в том числе от имени Банка, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену Банка: https://moscombank.ru или Системы ДБО https://dbo.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 Системы ДБО.

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

5. Не передавать логины, пароли, пин-коды и коды доступа другим лицам, в том числе сотрудникам Банка для проверки работоспособности или настройки Системы ДБО, хранить их в надежном месте, исключающем доступ к ним посторонних лиц. Вся ответственность за сохранность и использование паролей, логина, пин-кода иного кода доступа для доступа в Систему ДБО, полностью лежит на Клиенте как единственном их владельце.

6. Использовать виртуальную клавиатуру. Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками. Виртуальная клавиатура появляется при входе в Систему ДБО. При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе ДБО (если пароль содержит заглавную букву или символ, нажмите клавишу Shift, переключе-

ние между русским и английским алфавитом - клавиша Рус/Lat, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите Enter.

7. Исключить доступ посторонних лиц к компьютеру или мобильному устройству, использующемуся для работы в Системе ДБО. Осуществлять постоянный контроль отправляемых платежных электронных документов при работе в Системе ДБО, а также состояние своего личного счета.

8. Избегать работы в Системе ДБО 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 Систему ДБО.

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

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

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

12. В случае выявления явных или косвенных признаков компрометации Логина или Пароля, а также обнаружения вредоносных программ в компьютере, используемом для работы в Системе ДБО, 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:

- обнаружение факта или угрозы использования (копирования) идентификаторов учетной записи или паролей доступа к Системе ДБО неуполномоченных лиц (несанкционированная отправка электронных документов);
- обнаружение ошибок в работе Системы ДБО, в том числе возникающих в связи с попытками нарушения информационной безопасности;
- обнаружение воздействия вредоносного кода в компьютере, планшете, мобильном устройстве, мобильном телефоне, используемом для работы в Системе ДБО.

13. В случае выявления явных или косвенных признаков компрометации пароля учетной записи Клиент должен сменить данный пароль самостоятельно.

14. Обеспечивать конфиденциальность использования логина, паролей, пин-кодов, кодов доступа, которые не требуется сотрудникам Банка для обслуживания Клиента и поддержки Системы ДБО в работоспособном состоянии.

15. Применять на устройствах, используемых для работы Системы ДБО, лицензионные средства антивирусной защиты с возможностью автоматического обновления антивирусных баз и специализированные программные средства безопасности: персональные файерволы, антикейлоггеры, антиспам-фильтры.

16. Производить периодическую (не реже 1 раза в 3 месяца) смену долговременного пароля, а также по требованию Банка и в случае компрометации. Пароли должны выбираться исходя из следующих требований:

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

17. Самостоятельно убедиться, либо что используемое оборудование и программное обеспечение настроено для работы с сетью Интернет по защищенному протоколу https.

18. Не использовать на своем устройстве любые средства удаленного (дистанционного) доступа, которые обычно практикуют IT-специалисты для удаленной (дистанционной) поддержки (например, TeamViewer, AnyDesk, Ammy Admin и т.п.). Удалить или заблокировать возможность использования таких средств с помощью межсетевого экрана (программного и/или аппаратного).

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

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

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

22. Принимать звонки и СМС от Банка только номеров телефонов Банка: +74951090014, +73833358811.

В области социальной инженерии АО «МОСКОМБАНК» рекомендует Клиенту:

1. Обращать внимание на следующие признаки мошенничества:

- мошенник обращается с неизвестного номера телефона;
- мошенник представляется сотрудником Банка, Центрального Банка, Федеральных органов исполнительной власти (полиция, следователи, сотрудники Федеральной службы безопасности), операторов связи;
- Клиенту предлагается или какая-то выгода или описывается проблема и предлагается путь решения;

- от Клиента требуют сообщить номера карты, ПИН-код, логин и пароль от банковских приложений, подтвердить код по СМС, перейти по ссылке в СМС или e-mail сообщении, т.е. провести компрометацию конфиденциальных данных;
- от Клиента требуют провести мгновенную оплату, перевод денежных средств;
- от Клиента требуют быстрого принятия решения, немедленной реакции;
- возражают против того, чтобы Клиент позвонил позже, препятствуют разъединению телефонного звонка.

2. Учитывать следующие типичные случаи мошенничества:

Предложение мошенника	**Ваши действия**
Ваша карта заблокирована СМС-сообщение о якобы заблокированной карте, требуют сообщить ПИН-код или совершить действия в банкомате	Не переходите по ссылкам, перезвоните в Ваш банк. Помните, банк никогда не будет запрашивать номер карты, ПИН, иные коды
Родственник в беде Требование крупной суммы денег за решение проблем родственника, который якобы попал в беду. Мошенник представляется сотрудником полиции.	Обратите внимание на входящий телефон, наверняка он мобильный. Положите трубку и свяжитесь с Вашим родственником напрямую.
Требуется помощь в социальной сети Ваш знакомый по социальной сети описывает несчастье, которое случилось с ним или его родственниками, знакомыми и публикую номер карты/телефона, на которую идет сбор средств.	Перезвоните Вашему знакомому, не вступайте в переписку, аккаунт под контролем мошенника.
Выигрыш СМС/e-mail-сообщение о крупном выигрыше, предлагают перейти по ссылке	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вирусная атака СМС/ e-mail-сообщение содержит ссылку на какой-либо интернет ресурс, содержащий вредоносную программу, дающую доступ к карте	Не переходите по ссылке, наверняка на Ваше устройство будет установлено вредоносная программа
Вам положена компенсация Для получения компенсации Вам предлагают авансом оплатить пошлины, проценты, доставку, страховку и т.п.	Все предложения, требующие каких-то немедленных платежей являются мошенническими, положите трубку
Ошибочный перевод средств просят вернуть денежный средства за якобы ошибочный перевод	Не делайте поспешных действий, вначале проверьте действительно ли Вам приходила неизвестная сумма.
Карта заблокирована звонок «сотрудника банка», предлагают разблокировать карту, для чего просят сообщить реквизиты карты, код на обратной стороне, ПИН-код.	Положите трубку. Сотрудник банка не будет запрашивать реквизиты карты и коды.
«Сотрудник банка» проводит проверку данных или оказывает услугу и просит подтвердить «проверочный код»	Положите трубку, сотрудники банка не высылают никаких СМС-кодов. Если Вы подтвердите код с Вас спишут деньги.

«Вам по СМС должен поступить код, сообщите и проблема будет решена»	
Звонок из банка — просят перевести деньги на безопасный счет «Сотрудник банка» сообщает, что поступило заявление на закрытие счета, как будете забирать деньги. Потом говорят, что это мошенничество и предлагают сделать немедленно перевод на «безопасный счет», предлагают диктовать номер карты, ПИН-код, код на обратной стороне карты	Положите трубку, сотрудники банка не высылают никаких СМС-кодов.
Предоплата товара на сайте На различных площадках в интернете Вы обнаружили товар по привлекательной цене, но требуется перевод авансом на карту, по телефону.	Изучите продавца, отзывы о нем, историю, позвоните, предложите оплату при доставке. Ни в коем случае не оплачивайте авансы.
Просьба дать в долг От Ваших, друзей знакомых по социальной сети приходит просьба срочно прислать денег в долг	Перезвоните Вашему знакомому, уточните информацию. Не вступайте в переписку в этой же социальной сети, аккаунт Вашего знакомого скорее всего мошеннический.
Одобрение кредита «Сотрудник банка» сообщает об одобрении кредита на выгодных условиях. Для доступа к кредиту, надо внести плату за рассмотрение, за страхование, за выезд курьера и т. п. Плату внести предлагают через терминал/банкомат	Банк никогда не предлагает кредиты с предварительной оплатой каких-либо сопутствующих услуг.
Продление договора оператора связи «Сотрудник оператора связи» сообщает об окончании договора на мобильную связь и предлагает продлить его онлайн присылая ссылку, либо просит ввести код, который он уже выслал. В это время мошенник уже пытается взломать личный кабинетв ЕСИА «Госуслуги» и код это от двухфакторной аутентификации при входе на портал.	Немедленно положите трубку. Зайдите на портал ЕСИА «Госуслуги» и сбросьте пароль от входа. Позвоните на горячую линию портала ЕСИА «Госуслуги» и расскажите об инциденте для быстрой блокировки личного кабинете и смены пароля.

ПРИЛОЖЕНИЕ № 5 Заявление на возобновление ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

На основании Правил дистанционного банковского обслуживания частных клиентов в АО «МОСКОМБАНК» прошу Вас:

☐ - возобновить дистанционное банковское обслуживание моих счетов с ;

☐ - разблокировать, принадлежащую мне учетную запись в Системе 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 № 6 Заявление об изменении номера мобильного телефона

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ ОБ ИЗМЕНЕНИИ НОМЕРА МОБИЛЬНОГО ТЕЛЕФОНА

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

В соответствии Правилами дистанционного банковского обслуживания частных клиентов в АО «МОСКОМБАНК» прошу внести следующие изменения:

☐ - мой новый номер мобильного телефона + ( ) ;

в связи с

Подтверждаю, что данный телефонный номер, обслуживаемый оператором подвижной сотовой радиотелефонной связи, принадлежит мне на законных основаниях и может использоваться Банком для целей моей идентификации в Системе ДБО.

От Клиента _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

М.П.

ПРИЛОЖЕНИЕ № 7 Заявление на установление ограничений в Системе ДБО

МОСКОМБАНК
Commercial Bank of Moscow

ЗАЯВЛЕНИЕ НА УСТАНОВЛЕНИЕ ОГРАНИЧЕНИЙ В СИСТЕМЕ ДБО

Фамилия, имя, отчество (при наличии) Клиента

Реквизиты документа, удостоверяющего личность

Логин в Системе ДБО

Прошу АО «МОСКОМБАНК» установить следующие ограничения в Системе ДБО, рублей*:

- все переводы в сутки: 500 000,00;
- переводы по СБП в месяц: ****;**
- другие виды переводов _____ в сутки: **.**

* - для валютных счетов будет применяться ограничение, рассчитанное по курсу Банка России на день совершения операции.
** - данное ограничение может быть установлено только клиентам, признанным несостоятельными (банкротами).

Клиент _____ _____
подпись фамилия, инициалы

						2	0		

Отметки АО «МОСКОМБАНК»

Ограничения установлены.

Уполномоченный сотрудник Банка _____ _____
фамилия, инициалы подпись

						2	0		

ПРИЛОЖЕНИЕ № 8 Порядок обработки инцидентов

ПОРЯДОК ОБРАБОТКИ ИНЦИДЕНТОВ

1. Если у Вас есть подозрение, что Ваш **Пароль или Логин скомпрометированы, т.е. стали известны третьим лицам или утеряны,** либо произошло несанкционированное списание средств со Счета: незамедлительно выключите соответствующее устройство (компьютер, ноутбук, планшет, мобильный телефон и т.п.).

Если инцидент произошел в рабочее время Банка:

- Незамедлительно сообщите об инциденте по телефону Банка: +7 (495)109-00-14.
- Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении на регистрацию в Системе ДБО (Приложение № 1 к Правилам).
- После проведения аутентификации Банк незамедлительно осуществит блокировку Вашего Пароля и Идентификатора пользователя для входа в Систему ДБО, а также блокировку возможности проведения через Систему ДБО операций по Вашим счетам/картам, подключенным к Системе ДБО.

Если инцидент произошел в нерабочее время Банка:

- Если к Системе ДБО подключены банковские карты, незамедлительно позвоните в Процессинговый центр для блокировки счетов банковских карт: телефон Банка, который переадресует Ваш звонок на телефон Процессингового центра: +7 (495) 109-00-14.
- Незамедлительно примите меры для отзыва распоряжений на проведение расходных операций по Вашим счетам/картам, несанкционированных Вами. Для этих целей желательно использовать другое устройство (компьютер, ноутбук, планшет, мобильный телефон и т.п.).

2. Следует учитывать, что через Систему ДБО распоряжение может быть отозвано Клиентом в день его регистрации в Системе ДБО и только в том случае, если оно не исполнено, и Банк имеет возможность отменить его исполнение.

3. В других случаях неисполненное Банком распоряжение (если Банк имеет возможность его отзыва) может быть отозвано по Вашему звонку на телефон Банка: +7 (495) 109-00-14 в рабочее время Банка.

4. Если утерян либо похищен телефон (СИМ - карта) с номером, указанным в Заявлении о присоединении к Договору, незамедлительно сообщите об этом оператору сотовой связи для блокировки СИМ-карты.

5. Никогда и никому не сообщайте Ваш Пароль и Одноразовый пароль, включая сотрудников Банка.

6. Не сохраняйте Ваш Пароль и Логин на компьютере либо на других носителях электронной информации.

7. Внимательно проверяйте текст СМС-сообщения, которое содержит не только одноразовый Пароль, но также краткую информацию о совершаемой операции. Например, «19.02.2013 09:50:13 Ваш пароль номер 15: 0023216682 Perevod s 40817810203000006353 na 42306810300020001789».

8. Никогда не подтверждайте операцию одноразовым Паролем, если информация в СМС-сообщении не совпадает с операцией, которую Вы хотите подтвердить.

9. Не устанавливайте на мобильный телефон, на который Банк отправляет СМС-сообщения с одноразовым Паролем, приложения, полученные от неизвестных Вам источников. Банк никогда не рассылает своим клиентам ссылки и указания на установку приложений, за исключением приложений, размещённых самим Банком на официальном сайте или в официальных интернет-магазинах (репозиториях) интернет-приложений для AppStore, Google Play или на Сайте. Обязательно убедитесь, что разработчиком указан –

Закрытое акционерное общество «Центр финансовых технологий» (ЗАО «ЦФТ», JSC Center of Financial Technologies). При получении такого предложения от Банка незамедлительно в рабочее время Банка, сообщите об этом по телефону: +7 (495) 109-00-14.

10. По возможности, используйте в качестве устройства для получения СМС-сообщений от Банка простейший мобильный телефон, а не смартфон, поскольку риск заражения смартфона вредоносным программным обеспечением неизмеримо выше.

11. Не реже одного раза в день просматривайте выписки об операциях по счетам/картам, подключенным к Системе ДБО.

12. Для связи с Банком используйте только телефоны, указанные в настоящих Рекомендациях либо на официальном сайте в сети Интернет по адресу: www.moscombank.ru.

ПРИЛОЖЕНИЕ № 9 Политика конфиденциальности в Системе ДБО

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ В СИСТЕМЕ ДБО

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 Системы ДБО.

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 СИСТЕМЫ ДБО, включая Персональные данные.

Система ДБО – 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 Системе ДБО относятся: Интернет-банк (веб-версия, запускаемая через интернет-браузер по адресу https://dbo.moscombank.ru), Мобильное приложение (для смартфонов и планшетов). Обмен документами в электронной форме между Банком и Клиентом через сеть Интернет организован посредством информационно-технологического сервиса Faktura.ru, разработчиком которого является Закрытое акционерное общество «Центр финансовых технологий» (ИНН 5407125059, адрес 630055, Новосибирская область, Новосибирский район, рп Кольцово, д. 35), а разработчиком мобильных приложений – Закрытое акционерное общество «Центр цифровых сертификатов» (ИНН 5407187087, адрес 630055, Новосибирская область, г. Новосибирск, ул. Мусы Джалиля, д.11, каб. 309).

Интернет-банк - автоматизированная банковская система, обеспечивающая через информационно-телекоммуникационную сеть Интернет (далее - сеть Интернет) дистанционное банковское обслуживание (ДБО) Клиента посредством интернет-браузеров (веб-приложение) по адресу https://dbo.moscombank.ru.

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

Политика – настоящая Политика конфиденциальности.

Главное

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

Использование Клиентом Системы ДБО 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 Системы ДБО.

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 Системы ДБО, а также для проведения анализа и улучшения работы Системы ДБО; 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 Системы ДБО.

В Системе ДБО производится Обработка персональной информации следующих типов:

- информация, которую Клиент передает самостоятельно в процессе использования Системы ДБО, включая Персональные данные (например, при заполнении форм, заявок);
- информация, автоматически передаваемая в Банк в процессе использования Системы ДБО, 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 Системы ДБО;
- 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 Системы ДБО, в том числе сведений, составляющих банковскую тайну, Банк руководствуется Политикой, внутрибанковскими 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 персонифицированных сервисов;
- связь с Клиентом, в том числе направление уведомлений, запросов и информации, касающихся использования Системы ДБО, а также обработка запросов, заявок и распоряжений Клиента;
- 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 Системы ДБО. Данная информация используется для оптимизации Системы ДБО.

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 мобильного оператора, GPS, ГЛОНАСС, других систем геопозицинирования, Bluetooth, Wi-Fi, 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 Системы ДБО 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.