УТВЕРЖДЕНО ПРЕЗИДЕНТОМ
АО «МИДЗУХО БАНК (МОСКВА)»
Приказ № 84/22 от 14.12.2022 г.

# П Р А В И Л А

## предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

Москва

Декабрь 2022 / Редакция №10

Оглавление

## 1. Общие положения

1.1. Настоящие Правила оказания услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)» (далее – «Правила») являются неотъемлемой частью Договора о предоставлении услуг дистанционного банковского обслуживания (далее – «Договор») АО «Мидзухо Банк (Москва)» (далее – «Банк») и регламентируют порядок и условия:

- подключения и предоставления корпоративным клиентам (кроме кредитных организаций) услуг в системе дистанционного банковского обслуживания (далее – «система ДБО»);
- электронного документооборота в системе ДБО;
- рассмотрения конфликтных ситуаций, связанных с подлинностью электронных документов.
- обеспечения информационной безопасности в системе ДБО

1.2. Банк осуществляет предоставление услуг в системе ДБО в соответствии с Договором и Правилами, действующими на момент оказания услуги.

1.3. Информационный обмен в рамках системы ДБО осуществляется по открытым каналам связи с использованием сети Интернет.

1.4. Для подключения к системе ДБО Банка Клиент должен организовать рабочее место и подготовить персональный компьютер в соответствии с Требованиями к программно-аппаратному обеспечению автоматизированного рабочего места Клиента (Приложение 1 к настоящим Правилам).

1.5. В процессе эксплуатации системы ДБО Стороны самостоятельно выполняют необходимые мероприятия, обеспечивающие работоспособность своих автоматизированных рабочих мест, каналов связи и защиту ключей электронной подписи, паролей и ресурсов автоматизированных рабочих мест от несанкционированного доступа, на своей территории.

1.6. Обмен информацией между Банком и Клиентом производится путем передачи в Банк и приема из Банка электронных документов.

- Каждый электронный документ, передаваемый в Банк, должен быть подписан электронными подписями лиц, имеющих полномочия на совершении соответствующих действий.
- Каждый электронный документ, передаваемый Банком подписан электронной подписью Банка.
- Контроль прав абонентов, подписавших своей электронной подписью электронный документ, производится в автоматическом режиме в процессе обработки этого электронного документа в системе ДБО.
- Перечень электронных документов, используемых в системе ДБО, указан в Приложении 2 к настоящим Правилам

1.7. Электронный документ порождает права и обязанности Сторон по Договору, Договорам банковского счета, другим соглашениям, в рамках которых происходит взаимодействие с использованием системы дистанционного банковского обслуживания, если передающей Стороной электронный документ оформлен надлежащим образом, заверен корректными электронными подписями лиц, имеющих

полномочия на совершение соответствующих действий, и передан по системе дистанционного банковского обслуживания, а принимающей Стороной – получен.

1.8. Любые вложения в электронные документы (включая графические копии документов) в случае, если такие электронные документы подписаны электронной подписью, рассматриваются как обмен документами и представители Сторон, использующие ключи ЭП при отправке электронных документов, подтверждают идентичность графических копий оригиналам документов и несут ответственность за последствия использования таких документов другой Стороной.

Помимо этого, Клиент вправе отправлять по системе ДБО переводы документов с заверением электронной подписью.

1.9. Период действия ключей электронной подписи абонентов системы ДБО устанавливается равным 13 (тринадцати) месяцам, но не более срока действия полномочий Абонента. Абоненты обязаны самостоятельно осуществлять плановую смену ключей электронной подписи в соответствии с порядком, изложенным в разделе 4 настоящих Правил.

1.10. Банк осуществляет обработку персональных данных уполномоченных лиц Клиента в целях предоставления Клиенту услуг в системе дистанционного банковского обслуживания Банка и обеспечивает их защиту в соответствии с действующим законодательством. Клиент обеспечивает наличие согласия уполномоченных лиц Клиента на обработку и передачу Банку их персональных данных.

## 2. Термины и определения

2.1. **Абонент системы ДБО (Абонент) –** зарегистрированное в системе ДБО уполномоченное Клиента, владеющее ключами ЭП, сертификаты которых зарегистрированы в реестре Удостоверяющего Центра Банка, и уполномоченное осуществлять некоторые или все перечисленные действия с электронными документами: создание, подписание, прием и передача.

2.2. **Автоматизированное рабочее место (АРМ) системы ДБО** – программно-аппаратный комплекс, в состав которого входит программное обеспечение, предназначенное для подготовки, приёма/передачи и последующей обработки электронных документов, а также программное обеспечение системы криптографической защиты передаваемых электронных документов.

2.3. **Администратор системы ДБО** - уполномоченный сотрудник Банка, отвечающий за функционирование и работоспособность системы ДБО.

2.4. **Запрос на сертификат открытого ключа ЭП (запрос на сертификат) -** электронный файл, содержащий открытый ключ ЭП абонента системы ДБО, информацию об этом абоненте, а также вспомогательную информацию, на основе которой Банком формируется сертификат открытого ключа ЭП.

2.5. **Квитанция** – электронный документ, который формируется подтверждающей Стороной, содержащий информацию о статусе обработки подтверждаемого электронного документа.

2.6. **Клиент** – клиент Банка, заключивший с Банком Договор о предоставлении услуг дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)».

2.7. **Ключ электронной подписи (Ключ ЭП)** - уникальная последовательность символов, предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.

2.8. **Ключ проверки электронной подписи (Открытый ключ ЭП)** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

2.9. **Компрометация ключа ЭП** – событие, в результате которого становится возможным использование ключа электронной подписи неуполномоченным лицом. К событиям, влекущим компрометацию электронного ключа, в том числе, относятся следующие:

2.9.1. утрата носителей ключевой информации;

2.9.2. утрата (в том числе хищение) носителей ключевой информации с последующим обнаружением их местонахождения;

2.9.3. передача ключа ЭП по линии связи в открытом виде;

2.9.4. нарушение правил хранения носителей ключевой информации;

2.9.5. возникновение подозрений о несанкционированном распространении информации в системе ДБО или ее искажении;

2.9.6. отрицательный результат при проверке ЭП;

2.9.7. нарушение целостности упаковки ключевых носителей;

2.9.8. несанкционированное копирование носителей ключевой информации;

2.9.9. другие события, определенные Клиентом, как ознакомление неуполномоченным лицом (лицами) с ключами ЭП.

События, указанные в п.п. 2.9.1 – 2.9.4 должны трактоваться как безусловная компрометация действующих ключей. События, указанные в п.п. 2.9.5 – 2.9.9 не могут однозначно трактоваться как безусловная компрометация ключа и требуют специального расследования в каждом конкретном случае.

2.10. **Копия электронного документа (ЭД)** - электронный документ, полученный в результате копирования исходного (копируемого) электронного документа встроенными средствами системы ДБО, идентичный по содержанию исходному электронному документу, но имеющий иной, нежели исходный электронный документ, уникальный идентификатор в системе ДБО.

2.11. **Некорректный электронный документ (ЭД)** - электронный документ, получивший отрицательный результат при проведении проверки (не прошедший проверку) по одной или нескольким из следующих процедур:

- расшифровывания;
- подтверждения подлинности ЭП;
- контроля правильности заполнения полей документа

2.12. **Носитель ключевой информации (ключевой носитель)** – информационный носитель, содержащий ключ электронной подписи и ключ проверки электронной подписи.

2.13. **Подтверждение подлинности ЭП в электронном документе -** положительный результат проверки принадлежности ЭП абоненту системы ДБО средствами криптографической защиты информации (СКЗИ) с использованием сертификата ключа ЭП.

2.14. **Сертификат ключа проверки электронной подписи (Сертификат открытого ключа ЭП, Сертификат ЭП) -** электронный документ или документ на бумажном носителе, выданные Удостоверяющим Центром Банка и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.15. **Система криптографической защиты информации (СКЗИ) в системе ДБО** – специализированное программное обеспечение, используемое в системе ДБО Банка для создания ЭП, проверки подлинности ЭП, шифрования и расшифровывания передаваемых по системе электронных документов.

2.16. **Средства электронной подписи** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

2.17. **Удостоверяющий центр банка –** организационное подразделение Банка, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронной подписи, ведение реестра сертификатов ключей проверки электронной подписи и другие функции, предусмотренные Федеральным законом 63-ФЗ «Об электронной подписи».

2.18. **Электронный документ (ЭД)** – документ, в котором информация представлена в электронно-цифровой форме.

2.19. **Электронная подпись (ЭП)** – информация в электронной форме, которая присоединена к электронному документу или иным образом связана с электронным документом и которая используется для определения лица, подписывающего информацию. В рамках настоящих Правил под электронной подписью понимается усиленная неквалифицированная электронная подпись в терминах Федерального законом от 06.04.2011 №63-ФЗ «Об электронной подписи». Электронная подпись формируется в результате криптографического преобразования информации с использованием ключа электронной подписи; электронная подпись позволяет определить лицо, подписывающее документ; электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после его подписания и создается с использованием средств электронной подписи.

2.20. **Шифрование** - способ преобразования открытой информации в закрытую и обратно. Применяется для хранения важной информации в ненадёжных источниках или передачи её по незащищённым каналам связи. Шифрование подразделяется на процесс зашифровывания и расшифровывания.

## 3. Порядок подключения к системе ДБО

3.1. По запросу Клиента Банк подготавливает и направляет клиенту для подписания Договор о предоставлении услуг дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)» (далее - Договор).

3.2. Клиент подписывает Договор и направляет его в Банк.

3.3. Для каждого уполномоченного лица Клиент заполняет Заявление на регистрацию Абонента системы ДБО (Приложение 3 к настоящим Правилам) и направляет его в Банк.

3.4. В течение 3-х рабочих дней после получения Заявления на регистрацию Абонента системы ДБО, Банк проводит необходимую работу по регистрации Клиента в системе ДБО и подготовке необходимых Абонентам Клиента средств доступа к системе.

3.5. Уполномоченный представитель Клиента, действующий на основании надлежащим образом оформленной доверенности (образец доверенности указан в Приложение 4 к настоящим Правилам) либо Руководитель организации Клиента, прибывает в Банк для получения средств доступа к системе ДБО.

3.6. Представитель Банка передает средства доступа к системе ДБО представителю Клиента по Акту приема-передачи (Приложение 5 к настоящим Правилам). Акт приема-передачи средств ДБО составляется в 2 (двух) экземплярах по одному для каждой из Сторон.

3.7. В исключительных случаях, определяемых Банком, средства доступа к системе ДБО могут быть доставлены абонентам Клиента с использованием следующих альтернативных каналов:

3.7.1. Курьерской службой при соблюдении мер, исключающих бесконтрольный доступ во время доставки. Для пересылки комплекты средств доступа, а также документы, подлежащие подписанию Клиентом, помещаются в прочную упаковку (сейф-пакет). Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и печати. Возврат документов, подписанных Клиентом, осуществляется курьерской доставкой или по почте заказным почтовым отправлением.

3.7.2. При наличии у Клиента хотя бы одного Абонента ДБО имеющего доступ в систему ДБО, Банк вправе передавать идентификаторы доступа и пароли Абонентов данного Клиента, внутри зашифрованных файлов защищенных паролями, вложенных в произвольный документ системы ДБО.

При передаче идентификаторов доступа и паролей Абонентов по ДБО на каждого абонента ДБО формируется отдельный файл. Также Клиенту передается электронная версия Акта приема-передачи средств доступа к системе ДБО (Приложение 5 к настоящим Правилам)

3.7.3. В случае отсутствия действующих Абонентов ДБО, Банк вправе передавать пароли Абонентов данного Клиента внутри зашифрованных файлов, защищенных паролями, с использованием электронной почты по адресу, официально предоставленному клиентом в заявлении на регистрацию Абонента ДБО. При этом идентификатор доступа Абонента по электронной почте не передается.

При передаче паролей Абонентов по адресу электронной почты на каждого абонента ДБО формируется отдельный файл. Также Клиенту передается электронная версия Акта приема-передачи средств доступа к системе ДБО (Приложение 5 к настоящим Правилам).

При использовании электронных каналов передачи информации согласно пунктам 3.7.2 и 3.7.3 передача идентификатора доступа Абонента ДБО и/или пароля от файла производится Абоненту ДБО лично по телефону, указанному данным Абонентом в

Заявлении на регистрацию абонента ДБО. При этом до передачи пароля от зашифрованного файла Представитель Банка обязан дополнительно провести идентификацию данного Абонента путем запроса информации известной только данному Абоненту. Пароль сообщается Абоненту только в случае получения правильных ответов на запрошенную информацию.

После получения средств Доступа к системе ДБО Клиент обязан распечатать в 2-х экземплярах Акт приема-передачи средств доступа к системе ДБО, подписать уполномоченным сотрудником Клиента, поставить печать организации Клиента и направить Акты в Банк курьерской доставкой или заказным почтовым отправлением.

Для ускорения процесса получения доступа к системе отсканированный экземпляр Акта может быть направлен Клиентом на адрес электронной почты службы поддержки системы ДБО.

3.8. Подписание Акта приема-передачи средств доступа к системе ДБО подтверждает факт оказания услуги по регистрации Клиента в системе ДБО и является основанием для оплаты Клиентом вознаграждения за регистрацию Клиента в системе ДБО согласно Тарифам.

3.9. После получения средств доступа Абоненты Клиента самостоятельно инициируют процесс генерации собственных рабочих ключей ЭП и ключей проверки электронной подписи, отправки запросов на сертификат в Банк, получения и обработки сертификатов.

3.10. Процесс первоначального подключения к системе ДБО и действия, необходимые для формирования и регистрации собственных рабочих ключей электронной подписи описаны в Руководстве по установке, настройке и обновлению АРМ Клиента, доступной на сайте банка в сети Интернет по адресу http://www.mizuhobank.com/russia/ru/service/remotebanking.html.

3.11. В случае необходимости получения технической поддержки Клиент обращается в службу поддержки системы ДБО по телефонам Банка и/или по электронной почте support@mhcb.ru.

3.12. После получения запроса на сертификат ключа проверки ЭП абонента ДБО, уполномоченный сотрудник Удостоверяющего центра Банка проверяет соответствие информации в Заявлении на регистрацию Абонента системы ДБО, информации, содержащейся в запросе на сертификат. При положительном результате проверки создает сертификат ключа проверки ЭП, (Приложение 6 к настоящим Правилам), и распечатывает его в 2-х экземплярах

3.13. Выдача сертификата ключа проверки ЭП владельцу – абоненту системы ДБО производится в Банке, при личном присутствии абонента системы ДБО. При выдаче сертификата уполномоченный сотрудник Банка обязан провести идентификацию Абонента системы ДБО, на основании данных документа, удостоверяющего личность Абонента системы ДБО, либо его нотариально заверенной копии.

3.14. Банк вправе наделить полномочиями по вручению сертификатов ключей проверки ЭП Абонентам системы ДБО Единоличный исполнительный орган Клиента, для Абонентов системы ДБО, относящихся к данному Клиенту, на основании Доверенности, выданной Банком Единоличному исполнительному органу Клиента.

При совершении порученных Банком действий Единоличный исполнительный орган Клиента обязан идентифицировать владельца сертификата ключа проверки ЭП при его личном присутствии. При этом подписание Сертификата ключа проверки ЭП Единоличным исполнительным органом Клиента является безоговорочным подтверждением проведения идентификации владельца сертификата.

3.15. Не позднее следующего рабочего дня после получения экземпляра сертификата проверки ЭП, подписанного Клиентом, Администратор системы ДБО вводит сертификат ключа ЭП Абонента Клиента в действие. При этом оба экземпляра сертификата должны быть также подписаны Администратором системы ДБО, заверены подписью уполномоченного сотрудника и печатью Банка. Один подписанный Банком экземпляр сертификата возвращается Абоненту Клиента, второй остается на хранение в Банке.

3.16. До ввода в действие сертификата ключа проверки ЭП, доступ Абонента – владельца данного сертификата, в систему ДБО не предоставляется

3.17. Подключение новых Абонентов Клиента осуществляется в порядке, установленном в пунктах 3.3 - 3.15 настоящих Правил.

3.18. Изменение состава Абонентов Клиента имеющих право подписи электронных документов возможно только после направления в Банк оформленной должным образом новой карточки с образцами подписей и оттиска печати и иных документов, удостоверяющих полномочия Абонентов.

3.19. В случае изменения области действия ключа ЭП для зарегистрированных Абонентов, Клиент оформляет и предоставляет в банк Заявление на изменение области действия ключа электронной подписи Абонента системы ДБО по форме Приложения 9 настоящих Правил.

## 4. Порядок проведения плановой смены (перегенерации) ключа ЭП

4.1. Срок действия ключей ЭП в системе ДБО устанавливается равным 13 (тринадцати) месяцам.

4.2. За 30 (тридцать) календарных дней до истечения срока действия ключа ЭП абонента Клиента система ДБО при каждой загрузке предлагает абоненту произвести плановую смену (перегенерацию) ключа ЭП. Если абонент Клиента соглашается произвести смену, то система ДБО осуществляет генерацию нового ключа электронной подписи, формирование запроса на сертификат и направление его в Банк через систему ДБО.

4.3. Если запрос на сертификат подписан корректной ЭП абонента Клиента, Удостоверяющим Центром Банка создается сертификат нового рабочего ключа ЭП абонента Клиента. Если Клиент не произвел своевременную плановую замену своих ключей ЭП, то у него прекращается возможность использования ключей ЭП для подписи электронных документов. В случае необходимости предоставления указанным абонентам Клиента права подписи электронных документов с использованием ключей ЭП Клиент должен повторно осуществить действия по регистрации Абонента в соответствии с пунктами 3.3 - 3.16 настоящих Правил.

4.4. Срок хранения сертификата ключа ЭП определяется в соответствии с законодательством Российской Федерации.

## 5. Порядок действий в случае компрометации ключа ЭП

5.1. При выявлении одной из Сторон признаков несанкционированного использования неуполномоченными лицами ключа ЭП (в том числе несанкционированного списания или попытки списания денежных средств со счета), Сторона, выявившая признаки несанкционированного использования неуполномоченными лицами ключа ЭП, должна незамедлительно уведомить другую Сторону о данном факте.

5.2. Действия в случае компрометации ключа ЭП Абонента Клиента.

5.2.1. Решение о компрометации ключа ЭП может быть принято Абонентом Клиента, на имя которого выпускался ключ ЭП, либо руководителем Клиента.

5.2.2. Работа на скомпрометированном ключе ЭП должна быть приостановлена немедленно после обнаружения факта компрометации ключа ЭП.

5.2.3. В случае принятия решения о компрометации ключа ЭП Клиент незамедлительно должен уведомить Банк по телефону о факте его компрометации. Банк вправе запросить дополнительную информацию для идентификации Абонента Клиента.

5.2.4. Получив предварительное сообщение по телефону о компрометации ключа ЭП, Банк немедленно приостанавливает обработку электронных документов, подписанных скомпрометированным ключом ЭП, до получения уведомления о компрометации ключа ЭП в форме документа на бумажном носителе или по системе ДБО.

5.2.5. В течение 1 (одного) рабочего дня, следующего за датой предварительного сообщения по телефону о компрометации ключа ЭП, Клиент должен предоставить в Банк Уведомление о компрометации ключа ЭП по форме Приложения 7 к настоящим Правилам (далее – Уведомление о компрометации). Уведомление о компрометации может быть направлено в Банк:

- на бумажном носителе, подписанное руководителем либо лицом, действующим на основании надлежащим образом оформленной доверенности в рамках предоставленных ему полномочий, и заверенное печатью Клиента;
- с использованием системы ДБО путем направления Уведомления о компрометации как вложение в электронный документ («произвольный документ в банк» в терминах системы ДБО) с указанием в поле «Тема» сообщения «Уведомление о компрометации ключей ЭП». Уведомление направляется с использованием действующих (нескомпрометированных) ключей, при их наличии у Клиента.

5.2.6. После получения сообщения о компрометации ключей ЭП Администратор системы ДБО должен заблокировать соответствующий сертификат в системе ДБО.

5.2.7. При необходимости Стороны проводят в соответствии с разделом 3 настоящих Правил процедуру создания и сертификации нового ключа ЭП абонента Клиента, ключ ЭП, которого был скомпрометирован.

5.2.8. Банк начинает приём и обработку электронных документов, подписанных новым рабочим ключом ЭП абонента Клиента, не позднее рабочего дня, следующего за днем получения от Клиента надлежащим образом оформленного Бланка регистрации сертификата ключа ЭП абонента Клиента.

5.2.9. При получении информации о возможной компрометации ключа Абонента Клиента не от Клиента, Администратор системы ДБО для подтверждения факта компрометации незамедлительно после получения им такой информации, связывается с Абонентом Клиента по телефону, указанному в Заявлении на изготовление сертификата ключа электронной подписи. В случае невозможности связаться с Абонентом Клиента в течение 15 (пятнадцати) минут, Банк вправе самостоятельно принять решение о блокировке соответствующего сертификата для предотвращения возможной фальсификации электронных сообщений.

5.3. Разблокировка ключа Абонента Клиента.

5.3.1. Разблокировка ключа Абонента Клиента возможна только в случае блокировки ключа по обстоятельствам, которые не могут однозначно трактоваться как безусловная компрометация ключа. Если в ходе проведённого в соответствии с п.2.10 расследования компрометация ключа не подтвердилась, ключ Абонента Клиента может быть разблокирован по Заявлению Клиента.

5.3.2. Заявление о разблокировке ключа составляется Клиентом в произвольной форме, подписывается Абонентом Клиента и направляется в Банк на бумажном носителе или в виде вложения по Системе ДБО с использованием действующих (нескомпрометированных) ключей. При отсутствии технической возможности воспользоваться системой ДБО Заявление может быть передано Клиентом в Банк по факсу или электронной почте с последующим обязательным направлением Заявления на бумажном носителе в Банк не позднее 1 (одного) рабочего дня. После направления Заявления в Банк, Абонент Клиента связывается со службой поддержки Банка по телефону и сообщает о направлении Заявления о разблокировке.

5.3.3. Для разблокировки ключа Абонента Клиента сотрудник Банка не позднее 2 (двух) рабочих часов после звонка Абонента Клиента и получения Банком соответствующего заявления Клиента, направленного в соответствии с п.5.3.2, связывается с Абонентом Клиента по телефонному номеру, указанному в Заявлении на изготовление сертификата ключа электронной подписи, и подтверждает действительность решения Клиента о разблокировке ключа. При этом Абонент Клиента должен сообщить ФИО абонента Клиента и серийный номер сертификата открытого ключа. Банк вправе запросить дополнительную информацию для идентификации Абонента Клиента.

5.3.4. Разблокировка ключа осуществляется в течение 2 (двух) рабочих часов после получения Заявления о разблокировке ключа на бумажном носителе, или подтверждения решения Клиента о разблокировке ключа в случае направления заявления по системе ДБО, а также посредством факса или электронной почты.

## 6. Порядок электронного документооборота в системе ДБО

6.1. Передача в системе ДБО электронных документов отличных от перечисленных в «Перечне электронных документов используемых в системе ДБО АО «Мидзухо Банк (Москва)»» (Приложение 2 к настоящим Правилам) не влечет возникновения

обязательств у Сторон за исключением случаев, специально оговоренных Сторонами в дополнительных соглашениях к Договору.

6.2. Каждый электронный документ оформляется передающей Стороной в соответствии с требованиями действующего законодательства Российской Федерации и нормативных актов Банка России. Ответственность за правильность оформления электронного документа несет отправитель.

6.3. Электронный документ может быть создан непосредственно в системе ДБО или подготовлен и импортирован из внешней системы. Информацию о совместимости системы ДБО Банка и внешней системы Клиента можно уточнить, обратившись в службу поддержки системы ДБО Банка.

6.4. Каждый электронный документ в системе ДБО имеет уникальный идентификатор, назначаемый системой при создании документа. Стороны согласны с тем, что электронные документы одного типа и содержания, подписанные одинаковыми ЭП, считаются разными в случае различия уникальных идентификаторов.

6.5. Электронный документ порождает у Сторон обязательства только в том случае, если он отвечает следующим условиям:

- Оформлен в соответствии с п. 6.2 настоящих Правил;
- Прошёл все необходимые виды контроля;
- Заверен действующими ЭП отправителя и подлинность данных ЭП подтверждена;
- Доставлен получателю.

6.6. Клиент обязан своевременно проверять наличие Квитанций от Банка и статус обработки всех переданных им электронных документах. Клиент вправе запросить в Банке дополнительные разъяснения в случае получения отказа в обработке переданного электронного документа.

6.7. Клиент вправе предоставить в Банк документы, указанные в Приложении 2 к настоящему Договору («Перечень электронных документов…»), оформленные на бумажных носителях в соответствии с требованиями действующего законодательства Российской Федерации и нормативных актов Банка России. В этом случае Клиент не должен дублировать их в системе ДБО.

6.8. Клиент вправе предоставить в Банк заявление на ограничение осуществления операций по счёту в системе ДБО, включая ограничение максимальной суммы одной операции и (или) операций за определенный период времени. Для подачи Клиент должен направить в Банк письменное заявление по форме Приложения 10.

6.9. Банк не несет ответственности за своевременность передачи электронного документа Клиентом Банку. Клиент обязуется самостоятельно осуществлять своевременную передачу и получение электронных документов.

6.10. Подготовка и отправка в Банк электронных документов осуществляется в следующем порядке:

6.10.1. Абонент Клиента производит подготовку ЭД, руководствуясь правилами, приведенными в пунктах 6.3 и 6.10 настоящих Правил, и сохраняет подготовленные ЭД в базе данных системы ДБО. Подготовленные и сохраненные ЭД получают статус «Новый».

6.10.2. Должностные лица – абоненты Клиента, обладающие правом подписи, подписывают ЭД Клиента с помощью принадлежащих им ключей ЭП. При этом

система ДБО автоматически проверяет корректность каждой ЭП. Если ЭП некорректна или абонент не имеет соответствующих полномочий, данная ЭП не сохраняется и ЭД считается неподписанным.

6.10.3. Если ЭД подписан необходимым количеством корректных ЭП, документ приобретает статус «Подписан».

6.10.4. Абонент Клиента выбирает из общего списка документов ЭД, подлежащие отправке и находящиеся в статусе «Подписан», и передаёт их на обработку в Банк.

6.10.5. Система ДБО последовательно проводит автоматический контроль корректности ЭП и реквизитов каждого ЭД. ЭД, успешно прошедший проверку на стороне Банка получает статус «Принят».

6.10.6. ЭД с некорректными ЭП и/или с ошибками реквизитов не принимаются Банком в обработку и остаются в прежнем статусе. АРМ Клиента отображает сообщение с расшифровкой ошибок.

6.10.7. Время присвоения ЭД статуса «Принят» считается временем поступления документа в Банк.

6.10.8. Присвоение ЭД статуса «Принят» не означает принятия Банком обязательства исполнить ЭД, т.к. документ к этому времени еще не прошел все виды банковского контроля.

6.11. Обработка электронного документа Клиента Банком:

6.11.1. Статус «Не принят» или «Отказан АБС» присваивается ЭД, если Банк не подтвердил по данному документу списание средств со счета Клиента. Причина отказа в исполнении документа Клиента доводится Банком в поле «Информация из Банка» электронного документа, либо в форме документа свободного формата (Произвольный документ из банка).

6.11.2. Статус «Исполнен» присваивается документу, если Банк подтвердил списание средств со счета Клиента (документ исполнен со счета Клиента).

6.11.3. При любых изменениях статуса ЭПД, перечисленных в настоящем разделе, Банк предоставляет Клиенту соответствующую Квитанцию.

6.12. Получение выписки по счету:

6.12.1. Ежедневно по рабочим дням до 11 часов по Московскому времени Банк формирует для Клиента выписки в виде электронных документов по всем счетам, обслуживаемым в системе ДБО. В выписке отражаются все операции, проведенные по счету Клиента за предыдущий операционный день Банка.

6.12.2. Клиент может запросить выписку по счёту путём передачи в Банк соответствующего электронного документа и автоматически получить из Банка сформированную выписку.

# 7. Порядок рассмотрения конфликтных ситуаций

## 7.1. Общие положения.

7.1.1. В данном разделе описан порядок разрешения конфликтных ситуаций между Клиентом и Банком, связанных с подлинностью электронных документов. Рассматриваются конфликтные ситуации двух типов:

- отказ Стороны от электронного документа (Сторона утверждает, что ее абонент не подписывал принятый другой Стороной электронный документ, а другая Сторона утверждает обратное);
- отказ Стороны от факта получения электронного документа (Сторона утверждает, что посланный ею электронный документ был принят другой Стороной, а другая Сторона это отрицает).

7.1.2. Сторона – инициатор рассмотрения конфликтной ситуации (далее – «Инициатор») должна подготовить и направить другой Стороне (далее – «Ответчик») документ (заявление), подписанный уполномоченным должностным лицом, с изложением обстоятельств случившегося. До подачи заявления Заявителю рекомендуется убедиться в неизменности используемой ЭП, а также отсутствии несанкционированных действий со стороны персонала. В заявлении должно быть указано:

- наименование организации;
- дата, номер и тип оспариваемого электронного документа;
- тип и характер претензии.

7.1.3. На основании заявления Ответчик в течение 5 (пяти) рабочих дней рассматривает заявление, и либо удовлетворяет претензию Заявителя, либо передает Заявителю письменный отказ в удовлетворении претензии с обоснованием причины отказа.

7.1.4. В случае несогласия с отказом Инициатор направляет Ответчику письменное заявление о своем несогласии и требованием формирования экспертной комиссии для рассмотрения конфликтной ситуации.

7.1.5. На основании данного заявления, не позднее 15 (пятнадцати) календарных дней с момента его получения, совместным решением Сторон создается экспертная комиссия для рассмотрения возникшей конфликтной ситуации. Представителями в экспертной комиссии от Инициатора и Ответчика могут быть лица, как из числа сотрудников этих организаций (в равном количестве от каждой Стороны), так и иных компетентных организаций. В последнем случае их полномочия определяются доверенностями. Состав экспертной комиссии согласовывается Сторонами и утверждается двусторонним актом.

7.1.6. Рекомендуется следующий состав экспертной комиссии:

- абоненты, участвовавшие в обмене электронными документами, со стороны Инициатора и Ответчика;
- представители подразделений безопасности и технических подразделений Инициатора и Ответчика.

Кроме того, в случае необходимости, могут привлекаться независимые эксперты и технические специалисты иных компетентных организаций, в том числе организаций-изготовителей используемого программного обеспечения.

7.1.7. В течение 5 (пяти) рабочих дней с момента формирования экспертной комиссии Стороны предоставляют экспертной комиссии следующие материалы:

- заявление Инициатора с изложением сути претензии;
- письменный отказ Ответчика в удовлетворении претензии Инициатора;
- оспариваемые электронные документы, подписанные ЭП, а также квитанции на эти электронные документы;

- заверенные Бланки регистрации сертификатов ключей ЭП абонентов Сторон и сами сертификаты с использованием которых формировалась ЭП спорного электронного документа и ЭП квитанции на него в электронном виде на дискетах или иных носителях информации;

7.1.8. Кроме того, Банк предоставляет экспертной комиссии:

- эталонную ПЭВМ (персональный компьютер, свободный от вирусов и программных закладок) для автоматизированного рабочего места разбора конфликтной ситуации;
- полученный от производителя средств ЭП инсталляционный комплект эталонного ПО, предназначенного для проверки ЭП оспариваемого электронного документа;
- другие материалы, имеющие отношение к сути рассматриваемой претензии.

7.1.9. Стороны обязаны способствовать работе экспертной комиссии и своевременно предоставлять все необходимые материалы.

7.1.10. Экспертная комиссия на территории Банка рассматривает спорную ситуацию. При этом проверка корректности ЭП на оспариваемых электронных документах осуществляется в следующем порядке:

7.1.10.1. в присутствии членов экспертной комиссии Администратор системы ДБО Банка устанавливает на автоматизированное рабочее место разбора конфликтной ситуации (эталонную ПЭВМ) эталонное ПО с предоставленного экспертной комиссии инсталляционного комплекта;

7.1.10.2. экспертная комиссия убеждается в работоспособности эталонного ПО;

7.1.10.3. экспертная комиссия с помощью эталонного ПО производит проверку корректности ЭП, которой подписан оспариваемый электронный документ;

7.1.10.4. экспертная комиссия не позднее 10 (десяти) рабочих дней после получения всех материалов, указанных в пункте 7.1.7 настоящих Правил, большинством голосов членов принимает решение о виновности той или иной Стороны и оформляет его в виде акта, который оформляется на бумаге и подписывается всеми членами экспертной комиссии.

7.1.11. Акт экспертной комиссии является окончательным и пересмотру не подлежит. Предписываемые данным актом действия обязательны для Сторон.

7.1.12. Акт экспертной комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта.

7.1.13. В случае невозможности принятия решения экспертной комиссией, а также в случае несогласия одной из Сторон с принятым экспертной комиссией решением, уклонения одной из Сторон от формирования экспертной комиссии, препятствования участию второй Стороны в работе экспертной комиссии, Стороны вправе передать спор на рассмотрение в Арбитражный суд г. Москвы.

### 7.2. Порядок разрешения конфликта в связи с отказом Стороны от факта направления/подписания электронного документа.

7.2.1. В данном разделе описана процедура разрешения конфликта, вызванного отказом одной из Сторон от электронного документа: Инициатор утверждает, что его

абонент не подписывал принятый и исполненный Ответчиком электронный документ, а Ответчик утверждает обратное.

7.2.2. Запрашивается спорный электронный документ от Ответчика. В случае отказа Ответчика предоставить спорный электронный документ - конфликт разрешается в пользу Инициатора.

7.2.3. Проверяется корректность ЭП абонента для предоставленного электронного документа в соответствии с пунктом 7.4 настоящих Правил. Если ЭП признается некорректной, конфликт разрешается в пользу Инициатора.

7.2.4. В остальных случаях конфликт разрешается в пользу Ответчика.

### 7.3. Порядок разрешения конфликта в связи с отказом Стороны от факта получения электронного документа.

7.3.1. В данном разделе описана процедура разрешения конфликта, вызванного отказом одной из Сторон от факта получения электронного документа: Инициатор утверждает, что созданный им электронный документ с корректными ЭП в соответствии с правилами эксплуатации системы ДБО был передан Ответчику и принят последним, а Ответчик отрицает факт приема данного электронного документа.

7.3.2. Запрашивается спорный электронный документ и соответствующая ему квитанция о его доставке от Инициатора. В случае отказа предъявить спорный электронный документ или квитанцию о его приеме конфликт разрешается в пользу Ответчика.

7.3.3. Проверяется корректность ЭП абонента Инициатор в электронном документе в соответствии с пунктом 7.4 настоящих Правил. В случае некорректности ЭП конфликт разрешается в пользу Ответчика.

7.3.4. Проверяется корректность ЭП абонента Ответчика в квитанции в соответствии с пунктом 7.4 настоящих Правил. В случае некорректности ЭП конфликт разрешается в пользу Ответчика.

7.3.5. Проверяется соответствие квитанции электронному документу. В случае несоответствия квитанции электронному документу конфликт разрешается в пользу Ответчика.

7.3.6. В остальных случаях конфликт разрешается в пользу Инициатора.

### 7.4. Порядок проверки корректности электронной подписи на электронном документе.

7.4.1. В данном разделе описана процедура проверки корректности ЭП абонента для электронного документа. Данная процедура используется при разрешении вопроса о подлинности электронных документов или квитанций на них.

7.4.2. От Стороны, предоставившей электронный документ, запрашивается сертификат ключа ЭП, с использованием которого была сформирована ЭП для спорного электронного документа и/или квитанции. Проверяется ЭП спорного электронного документа на автоматизированном рабочем месте разбора конфликтных ситуаций в соответствии с пользовательской документацией системы ДБО. Если программа

не признает ЭП корректной на момент её создания, то принимается решение о некорректности ЭП электронного документа.

7.4.3. Если у одной из Сторон возникают сомнения в принадлежности сертификата ключа ЭП абоненту, производится процедура проверки принадлежности этого сертификата в соответствии с пунктом 7.5 настоящих Правил.

7.4.4. В случае если сертификат признается не принадлежащим данному абоненту, ЭП ЭД признается некорректной.

7.4.5. В остальных случаях принимается решение о корректности ЭП абонента для электронного документа.

### 7.5. Порядок проверки принадлежности сертификата абоненту.

7.5.1. В данном разделе описана процедура проверки принадлежности абоненту сертификата ключа ЭП.

7.5.2. Для проверки принадлежности сертификата абоненту у Банка запрашивается заверенный экземпляр Бланка регистрации сертификата ключа ЭП этого Абонента.

7.5.3. Проверяется соответствие сертификата ключа ЭП абонента данным Бланка регистрации. По результатам проверки принимается решение о принадлежности или не принадлежности сертификата Абоненту.

## 8. Обеспечение информационной безопасности в системе ДБО

### 8.1. Общие положения

8.1.1. Стороны обязуются принимать адекватные меры для защиты конфиденциальной информации в системе ДБО.

8.1.2. Стороны признают обязательным использование дополнительного средства аутентификации в системе ДБО при помощи одноразовых паролей для Абонентов Клиента, обладающих правом подписи.

8.1.3. Соблюдение требований информационной безопасности при организации обмена электронными документами обеспечивает:

- конфиденциальность информации (получить доступ к информации могут только уполномоченные лица);
- целостность передаваемой информации (гарантирование, что данные передаются без искажений и исключается возможность подмены информации);
- аутентификацию (возможность получения передаваемой информации только тем лицом, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

8.1.4. Требования по информационной безопасности при организации обмена электронными документами регламентированы законодательством Российской Федерации, нормативными документами Банка России, ФСБ России и реализуются посредством применения программно-технических средств и организационных мер.

8.1.5. К программно-техническим средствам относятся:

- программные средства системы ДБО;
- система паролей и идентификаторов для ограничения доступа пользователей и операторов к техническим и программным средствам системы ДБО;
- средства криптографической защиты информации;
- программно-аппаратные средства защиты от несанкционированного доступа;
- средства защиты от компьютерных вирусов;
- средства защиты от атак на вычислительные системы.

8.1.6. К организационным мерам относятся:

- размещение технических средств в помещениях с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- задание режима использования пользователями и операторами паролей и идентификаторов;
- допуск к осуществлению обмена электронными документами только специально обученных и уполномоченных на то лиц;
- поддержание программно-технических средств в исправном состоянии;
- резервирование программно-технических средств;
- обучение технического персонала;
- защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).

## 8.2. Обеспечение безопасности СКЗИ и ключевых носителей

8.2.1. СКЗИ, эксплуатационная и техническая документация к ним, лицензии, носители ключевой информации подлежат поэкземплярному учету в специально выделенных для этих целей журналах.

8.2.2. В качестве носителя ключевой информации должен быть использован только поддерживаемый системой внешний отчуждаемый носитель (USB-ключ РУТОКЕН ЭЦП, USB флеш накопитель). В целях защиты ключевой информации от несанкционированного доступа Банк рекомендует использовать в качестве ключевых носителей специально предназначенные для этого устройства, с реализацией криптографических алгоритмов непосредственно на ключевом носителе (USB-ключ РУТОКЕН ЭЦП).

8.2.3. Дистрибутивы СКЗИ на информационных носителях, эксплуатационная и техническая документация к СКЗИ, ключевые носители должны храниться в шкафах (сейфах, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

8.2.4. Допускается хранение носителей ключевой информации в хранилище, используемом совместно с другими сотрудниками, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца носителей ключевой информации и исключающей возможность негласного доступа к ним посторонних лиц.

8.2.5. При выявлении сбоев или отказов в работе СКЗИ или ключевых носителей Абонент обязан незамедлительно сообщить о факте их возникновения в службу поддержки системы ДБО Банка.

8.2.6. Абоненту ЗАПРЕЩАЕТСЯ:

- осуществлять несанкционированное копирование криптографических ключей;
- оставлять (даже на минимальное время) ключевые носители установленными в компьютер, если Абонент их не использует, или в открытом доступе (например, на столе);
- использовать ключевые носители для шифрования и подписи электронных документов, не относящейся к работе в системе ДБО Банка;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить Ключ ЭП на дисплей и/или принтер;
- вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ, а также в устройства считывания персональных компьютеров, не предназначенных для работы с системой ДБО Банка;
- записывать на носители с криптографическими ключами постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение СКЗИ.

## 8.3. Обеспечение безопасности средств доступа к системе ДБО

8.3.1. Абонентам системы ДБО рекомендуется:

- Не допускать использования простых паролей (123456, qwerty и др.) – используйте различные сложные комбинации из букв (в т.ч. в разных регистрах) и цифр, не расположенных «подряд» на клавиатуре.
- Осуществлять регулярную (минимум – 1 раз в месяц) смену паролей, используемых в системе ДБО.
- Не использовать для доступа к системе ДБО пароль, используемый в любых других системах и сервисах.
- Незамедлительно менять пароль и осуществлять перегенерацию ключей ЭП (используя соответствующие возможности системы ДБО) или обращаться в Банк для получения новых средств доступа в следующих случаях:
  - При увольнении сотрудника, имевшего доступ к ключам ЭП;
  - При возникновении любых подозрений на компрометацию ключей ЭП и/или средств доступа.
  - В случае обнаружения какого-либо вредоносного программного обеспечения на компьютере, используемом для работы в системе ДБО.

8.3.2. Абонентам системы ДБО категорически запрещено сообщать идентификатор доступа (логин) или пароль, используемый в системе ДБО, кому-либо, в том числе техническим специалистам для проверки работы системы, настроек

взаимодействия с Банком и др. При необходимости таких проверок владелец средств доступа обязан лично вводить свои логин и пароль в системе ДБО.

## 8.4. Обеспечение безопасности АРМ системы ДБО

8.4.1. Клиент, эксплуатирующий АРМ, должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства АРМ, изменение их состава, появление на АРМ и в системе ДБО компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения системы ДБО, электронных документов, либо на перехват паролей, ключей ЭП и другой конфиденциальной информации.

8.4.2. Рекомендуется оборудовать АРМ системы ДБО средствами контроля вскрытия.

8.4.3. На АРМ должен быть реализован комплекс мер и средств защиты от угроз публичной сети Интернет, обеспечивающий защиту данных от несанкционированного доступа по сети. Клиент, эксплуатирующий АРМ, должен постоянно использовать антивирусное программное обеспечение и своевременно осуществлять его обновление.

8.4.4. Рекомендуется применять специализированные программные средства безопасности: межсетевые экраны (Firewall), антишпионское программное обеспечение (Anti-Spyware software) и другое специализированное программное обеспечение, использующееся для обеспечения ИТ-безопасности.

8.4.5. Клиент должен обеспечить своевременную загрузку и установку обновлений операционной системы АРМ, а также регулярное обновление другого системного и прикладного программного обеспечения по мере появления их новых версий.

8.4.6. Рекомендуется создать на АРМ системы ДБО доверенную среду:

- Не устанавливать программы из непроверенных источников.
- Не загружать программы с «файлообменных» сайтов.
- Настоятельно рекомендуется не использовать АРМ для обычной работы в сети Интернет и развлечений. Чаще всего вирусы и вредоносное ПО распространяются через сайты развлекательного характера.
- По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к необходимым ресурсам (в частности используемым системой ДБО).
- Осуществлять антивирусную проверку любых файлов и программ, загружаемых из сети Интернет либо полученных по электронной почте или на внешних носителях (дискеты, флеш-накопители, CD/DVD и др.).
- Отключить возможность «автоматического выполнения» для подключаемых устройств: флеш-накопителей, компакт-дисков. Многие вирусы проникают в систему путем автозапуска с флеш-накопителя или компакт-диска.
- Ограничить доступ к компьютеру персонала, не имеющего отношения к работе с системой ДБО.

- Не допускать работу под учётной записью Windows, имеющей права администратора - необходимо использовать учётную запись с ограниченными правами в операционной системе Windows, установленной на компьютере.
- Не допускать использования «пустых» или простых паролей (123456, qwerty и др.) для всех учётных записей, имеющих право входа в Windows, а также осуществлять периодическую смену паролей (рекомендуемая частота смены паролей – 1 раз в месяц).
- Наблюдать за всеми действиями сотрудников (в т.ч. технических специалистов), в течение всего времени выполнения ими каких-либо действий на компьютерах, используемых для работы с системой ДБО.

8.4.7. В качестве дополнительного средства защиты от внешних атак в системе ДБО может быть использована фильтрация запросов Абонентов Клиента:

- по внутренним и внешним IP-адресам АРМ Клиента;
- физическим (MAC) адресам сетевых карт АРМ Клиента.

Для каждого Абонента Клиента может быть задан список разрешенных IP и MAC адресов, с которых может быть выполнено соединение с системой ДБО.

8.4.8. Для включения фильтрации запросов Абонентов Клиента по IP и/или MAC адресам Клиент:

- Устанавливает для АРМ-ов Клиента постоянные (статические) IP адреса
- Направляет в Банк на бумажном носителе Заявление на включение фильтрации доступа к системе ДБО по форме Приложения 8 к настоящим Правилам.

## 8.5. Требования к помещениям, используемым для размещения АРМ системы ДБО и хранения ключевых носителей

8.5.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены АРМ системы ДБО или хранятся ключевые носители (далее режимные помещения), должны обеспечивать их сохранность.

8.5.2. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

8.5.3. Размещение, специальное оборудование, охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

8.5.4. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, должен предусматривать периодический контроль состояния технических средств охраны, если таковые имеются.

8.5.5. Двери режимных помещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей.

8.5.6. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию АРМ. Дубликаты ключей от хранилищ хранятся в специальном сейфе у руководителя организации Клиента.

8.5.7. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за эти хранилища.

### 8.6. Уничтожение ключей ЭП

8.6.1. Неиспользованные или выведенные из действия ключи ЭП подлежат уничтожению.

8.6.2. Уничтожение ключей ЭП на ключевых носителях производится Абонентом, которому принадлежат данные ключи.

8.6.3. Ключи ЭП уничтожаются путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования. Абонент Клиента при необходимости может обратиться в службу технической поддержки системы ДБО для получения консультации по вопросам уничтожения ключей ЭП.

## 9. Приостановление и прекращение использования системы ДБО

9.1. Клиент имеет право прекратить использование системы ДБО путем направления в Банк на бумажном носителе Заявления о расторжении Договора в произвольной форме.

9.2. Банк имеет право приостановить или прекратить использование Клиентом системы ДБО по собственной инициативе при нарушении Клиентом порядка использования системы ДБО, а также в иных случаях, предусмотренных Договором и законодательством Российской Федерации.

9.3. **В случае выявления Банком операций, соответствующих признакам осуществления перевода денежных средств без согласия Клиента**, Банк приостанавливает использование системы ДБО Абонентами Клиента, которые подписывали распоряжение о совершении выявленной операции, и совершает в отношении данного распоряжения действия, предусмотренные Общими условиями открытия и ведения счетов юридических лиц и индивидуальных предпринимателей – клиентов АО «Мидзухо Банк (Москва)» (далее Общих условий). При получении от Клиента подтверждения возобновления исполнения распоряжения в соответствии с

Общими условиями Банк возобновляет использование Абонентом Клиента системы ДБО. При неполучении от Клиента подтверждения возобновления исполнения распоряжения в соответствии с Общими условиями Банк возобновляет использование Абонентом Клиента системы ДБО по истечении двух рабочих дней после дня совершения им действий, предусмотренных Общими условиями.

## 10. Порядок внесения изменений в Правила

10.1. Изменения и дополнения в настоящие Правила и Приложения к ним, а также сроки и порядок вступления в силу вносимых в настоящие Правила изменений и дополнений публикуются на официальном сайте Банка в сети Интернет по адресу http://www.mizuhobank.com/russia/ru/service/remotebanking.html и считаются доведенными до сведения Клиентов со дня такой публикации.

10.2. Тексты настоящих Правил и всех изменений и дополнений к ним на бумажном носителе должны храниться Банком в течение 3-х (трёх) лет после прекращения их действия.

10.3. Клиент имеет право запрашивать копии текстов настоящих Правил и всех изменений и дополнений к ним на бумажном носителе. Указанные в настоящем пункте документы должны быть предоставлены Банком Клиенту в течение 15 рабочих дней после получения соответствующего письменного запроса Клиента.

Приложение 1 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

## ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОМУ ОБЕСПЕЧЕНИЮ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛИЕНТА

Персональный компьютер со следующими характеристиками:

- Операционная система Microsoft Windows 10, Windows 11 (русская или английская версия);
- Веб-браузеры: Microsoft Internet Explorer 11, Google Chrome, Mozilla Firefox;
- Наличие доступа к сети Интернет;
- Наличие свободного USB-порта.

Приложение 2 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

## ПЕРЕЧЕНЬ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ, ИСПОЛЬЗУЕМЫХ В СИСТЕМЕ ДБО

**Платежные документы**:
*(подписывают лица из карточки подписей)*

- Платежное поручение
- Валютный перевод
- Поручение на покупку иностранной валюты
- Поручение на продажу иностранной валюты
- Поручение на конверсию валют
- Распоряжение на списание средств с транзитного валютного счета

**Документы валютного контроля**:
*(подписывают лица из карточки подписей или лица по доверенности)*

- Справка о валютных операциях
- Справка о подтверждающих документах
- Паспорт сделки по контракту
- Паспорт сделки по кредитному договору
- Заявление о закрытии/переводе паспортов сделок

**Документы для заключения сделок**:
*(подписывают лица в соответствии с условиями Соглашения)*

- KL: предоставление кредитного транша
- KL: предоставление кредитного транша с плавающей процентной ставкой
- KL: пролонгация кредитного транша
- KL: досрочное погашение кредитного транша
- KL: присоединение кредитных траншей
- MLA: предоставление Кредита
- MLA: предоставление Кредита с плавающей процентной ставкой
- MLA: пролонгация Кредита
- MLA: досрочное погашение Кредита
- MLA: присоединение Кредитов
- MGA: выдача Банковской Гарантии
- MGA: выдача Банковской Гарантии в ФТС
- MGA: внесение изменений в Банковскую Гарантию
- DEP: размещение депозита
- DEP: размещение депозита без открытия счета
- DEP: досрочный возврат депозита
- DEP: досрочный возврат депозита без открытия счета

**Иные документы, используемые в системе ДБО**:
*(подписывают лица из карточки подписей)*

- Произвольный документ (текстовое информационное сообщение и/или вложение в электронный документ)

Приложение 3 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**ЗАЯВЛЕНИЕ**
**НА РЕГИСТРАЦИЮ АБОНЕНТА СИСТЕМЫ ДБО***

" _____" _____ 20__ г.

_____
(наименование организации)

в целях использования в системе ДБО АО «Мидзухо Банк (Москва)» просит зарегистрировать Абонента:

Должность.....
.....
Фамилия.....
Имя .....
Отчество (при наличии) .....
Данные документа, удостоверяющего личность .....
.....
Зарегистрирован по адресу .....
Тел. .....
e-mail .....

Область действия ключа электронной подписи:
(***в соответствии с правилами, указанными в Приложении 2 к Правилам)***

☐ Подписание электронных платежных документов и документов валютного контроля
☐ Подписание документов для заключения сделок
☐ Доступ к системе ДБО без права подписи электронных документов

Ключевой носитель:

☐ Новый USB-ключ РУТОКЕН
☐ Ранее выданный USB-ключ РУТОКЕН (серийный номер: _____) **
☐ Собственный носитель (USB flash)

Примечание: .....
.....

Абонент системы ДБО _____ _____
*(подпись)* *(фамилия и инициалы)*

Руководитель организации _____ _____
*(подпись)* *(фамилия и инициалы)*

М.П.

** Все поля заявления обязательны к заполнению*
***Возможно только в случае замены уполномоченного Абонента Клиента*

**Отметки Банка:**

Приложение 4 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**ДОВЕРЕННОСТЬ № _____**

_____ _____
наименование населенного пункта дата, месяц, год

_____
*(наименование организации)*

в лице _____, действующего на основании _____
*(должность, ФИО)*

настоящей доверенностью уполномочивает _____,
*(должность, ФИО)*

_____года рождения, паспорт серии _____ №_____,
*(дата рождения)*

выдан _____
*(кем и когда выдан)*

получать в АО «Мидзухо Банк (Москва)» средства доступа к системе дистанционного банковского обслуживания, для чего подписывать акты приема-передачи средства доступа к системе ДБО и выполнять иные действия, связанные с выполнением данного поручения.

Подпись лица, получившего доверенность _____ удостоверяю.

Настоящая доверенность выдана сроком на 30 (тридцать) дней без права передоверия.

_____ _____ _____
*(должность руководителя)* *(подпись)* *(фамилия и инициалы)*

М.П.

Приложение 5 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**АКТ**
**ПРИЕМА-ПЕРЕДАЧИ СРЕДСТВ ДОСТУПА К СИСТЕМЕ ДБО**

г. Москва «____» _____20___г.
(заполняется Банком)

Настоящий Акт составлен в том, что Акционерное общество «Мидзухо Банк (Москва)» (далее «Банк») в лице _____, действующего на основании _____, передал,

а _____
*(Полное наименование организации)*

(далее «Клиент») в лице _____,
*(должность, Ф.И.О).*

действующего на основании _____
*(наименование документа)*

в соответствии с условиями Договора о предоставлении услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)» от _____ г. № _____ принял средства доступа к системе ДБО Банка в составе:

| № п/п | Наименование | Количество |
|---|---|---|
| 1. | USB-ключ РУТОКЕН (перезапись) | |
| 2. | Автономный генератор одноразовых паролей eToken PASS | |
| 3. | USB-ключ РУТОКЕН | |
| 4. | Персональный идентификатор и пароль для доступа к системе ДБО | |
| 5. | Распечатка сертификата ключа ЭЦП Банка | |

| **БАНК** | **КЛИЕНТ** |
|---|---|
| _____ *(должность)* | _____ *(должность)* |
| _____ *(фамилия и инициалы)* | _____ *(фамилия и инициалы)* |
| _____ *(подпись)* | _____ *(подпись)* |
| М.П. | «____»_____ 20__г. М.П. |

**Отметки Банка:**
Получен ОПЕРУ
«___» _____ 20___г.

Приложение 6 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ**

г. Москва «____» _____20___г.

Наименование организации: _____

Данные ключа:

Алгоритм: .....
Начало срока действия: .....
Окончание срока действия: .....
Уникальный (серийный) номер ключа проверки ЭП: .....
ФИО владельца: .....
Используемое средство / стандарты ЭП: .....

Ключ проверки ЭП:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Данный сертификат ключа проверки электронной подписи выдан и зарегистрирован Удостоверяющим Центром АО «Мидзухо Банк (Москва)»

Администратор системы ДБО Банка

_____ / /

**БАНК**

_____
*(должность)*

_____
*(фамилия и инициалы)*

_____
*(подпись)*

«____»_____ 20__г.

М.П.

Владелец сертификата ключа проверки ЭП

_____ / /

**КЛИЕНТ**

_____
*(должность)*

_____
*(фамилия и инициалы)*

_____
*(подпись)*

«____»_____ 20__г.

М.П.

Приложение 7 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**УВЕДОМЛЕНИЕ**
**О КОМПРОМЕТАЦИИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ**

«___» _____20__г.

Настоящим

_____
*(полное наименование организации)*

уведомляет о компрометации ключей электронной подписи, принадлежащих следующим абонентам:

| № п/п | Фамилия, имя, отчество (полностью) | Серийный номер сертификата ключа ЭП | Причина компрометации |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| … | | | |

Контактное лицо: _____
*(должность, ФИО, телефон, E-Mail)*

_____ _____ _____
*(должность руководителя)* *(подпись)* *(фамилия и инициалы)*

М.П.

**Отметки Банка:**
Уведомление о компрометации ключа ЭП получено Банком, предоставленные Клиентом сведения проверил, подпись руководителя верна:

_____ _____ _____
*(наименование должности сотрудника Банка)* *(подпись)* *(фамилия и инициалы)*

«___» _____ 20___г.

Приложение 8 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**ЗАЯВЛЕНИЕ**
**НА ВКЛЮЧЕНИЕ ФИЛЬТРАЦИИ ДОСТУПА К СИСТЕМЕ ДБО**

«___» _____20__г.

Настоящим

_____
*(полное наименование организации)*

Просит включить фильтрацию доступа к системе ДБО для абонентов:

| № п/п | Фамилия, имя, отчество (полностью) | Разрешенные IP и/или MAC адреса |
|---|---|---|
| 1. | | |
| 2. | | |
| … | | |

Контактное лицо: _____
*(должность, ФИО, телефон, E-Mail)*

_____ _____ _____
*(должность руководителя)* *(подпись)* *(фамилия и инициалы)*

М.П.

---

**Отметки Банка:**
Заявление получено

_____ _____ _____
*(наименование должности сотрудника Банка)* *(подпись)* *(фамилия и инициалы)*

«___» _____ 20___г.

Приложение 9 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**ЗАЯВЛЕНИЕ**
**НА ИЗМЕНЕНИЕ ОБЛАСТИ ДЕЙСТВИЯ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ АБОНЕНТА СИСТЕМЫ ДБО**

" _____" _____ 20__ г.

_____
(наименование организации)

Для Абонента:

Фамилия.....

Имя .....

Отчество (при наличии) .....

Контактные данные:

Тел. .....

e-mail .....

Назначить область действия ключа электронной подписи:
(***в соответствии с правилами, указанными в Приложении 2 к Правилам)***

☐ Подписание электронных платежных документов и документов валютного контроля
☐ Подписание документов для заключения сделок
☐ Доступ к системе ДБО без права подписи электронных документов

Примечание: .....
.....

Руководитель организации _____ _____
*(подпись)* *(фамилия и инициалы)*

М.П.

**Отметки Банка:**

Приложение 10 к Правилам предоставления услуг в системе дистанционного банковского обслуживания АО «Мидзухо Банк (Москва)»

**ЗАЯВЛЕНИЕ**
**НА ОГРАНИЧЕНИЕ ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ**

" _____" _____ 20__ г.

Настоящим

_____

*(полное наименование организации)*

Просит внести следующие ограничения операций по счетам в системе ДБО:

| Номер счета | Максимальная сумма одного документа (в валюте счета) | Максимальная сумма за период (в валюте счета) | Период в днях |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

Примечание: .....
.....

Руководитель организации _____ _____
*(подпись)* *(фамилия и инициалы)*

М.П.

**Отметки Банка:**