МТИ-Банк

07/02-11/9

ПРАВИЛА ОРГАНИЗАЦИИ И ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ в системе ДБО «МТИ-Банк» (АО) для юридических лиц и индивидуальных предпринимателей.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила организации и осуществления обмена электронными документами в системе ДБО «МТИ-Банк» (АО) для юридических лиц и индивидуальных предпринимателей (далее – Правила) разработаны в соответствии с законодательством Российской Федерации и иными нормативными актами.

1.2. Настоящие Правила являются публичным предложением (офертой) Банка заключить Договор об электронных расчетах с использованием Системы дистанционного банковского обслуживания на определенных Правилами условиях. Присоединение к Правилам производится в соответствии со ст. 428 Гражданского кодекса Российской Федерации для чего заинтересованное лицо, с учетом п. 1.4 настоящих Правил, должно представить в Банк надлежащим образом заполненную и подписанную Заявку на подключение к Системе ДБО, установленной Банком формы, а также иные необходимые документы и информацию.

1.3. Договор об электронных расчетах считается заключенным с момента проставления на Заявке на подключение к Системе ДБО подписи уполномоченным сотрудником Банка.

1.4. Настоящие Правила не регулируют обмен Банка электронными документами с кредитными организациями и физическими лицами, не являющимися индивидуальными предпринимателями или не занимающимися в установленном законодательством Российской Федерации порядке частной практикой.

1.5. Если не указано иное, термины и определения, применяемые в тексте настоящих Правил, означают следующее:

Автоматизированное рабочее место (АРМ) – комплекс программно-технических средств, используемых Клиентом для обмена ЭД;

Банк – «Межрегиональный торгово-инвестиционный банк» (Акционерное общество), являющийся оператором Системы;

Владелец ЭП – физическое лицо, указанное в Карточке с образцами подписей и оттиска печати Клиента, уполномоченное распоряжаться денежными средствами, находящимися на Счете, с использованием Системы, Ключ проверки ЭП которого зарегистрирован в Системе, или физическое лицо, уполномоченное Клиентом получать информацию в Системе без права распоряжаться денежными средствами, находящимися на Счете с использованием Системы, в случае использования просмотрового ключа ЭП, ключ проверки которого зарегистрирован в Системе;

Договор об электронных расчетах с использованием Системы ДБО (Договор об электронных расчетах, Договор) – совместно представленная Клиентом Заявка на подключение к Системе ДБО установленной Банком формы и настоящие Правила;

Документация – документация по установке и эксплуатации Системы и средств ЭП;

Дополнительное подтверждение – подтверждение корректности поступившего в Банк ЭПД Клиента посредством введения кода подтверждения, полученного владельцем ЭП в виде SMS-сообщения;

Индивидуальный предприниматель – непосредственно индивидуальный предприниматель, а также физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой;

Клиент – юридическое лицо или индивидуальный предприниматель, заключившее (заключающее) с Банком Договор об электронных расчетах в порядке, предусмотренном настоящими Правилами;

Ключ ЭП – уникальная последовательность символов, предназначенная:

- в полнофункциональном режиме – для создания электронной подписи электронного документа с использованием средств ЭП;
- в просмотровом режиме (Просмотровый ключ ЭП) – только для получения информации в Системе;

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с Ключом ЭП, предназначенная для проверки подлинности с использованием средств ЭП:

- в полнофункциональном режиме – электронной подписи электронного документа;
- в просмотровом режиме – Просмотрового ключа ЭП;

Кодовое слово – заявленное Клиентом в Банк слово, используемое Банком для подтверждения того, что обратившееся в Банк по телефону с заявлением о компрометации лицо является представителем Клиента. Кодовое слово используется исключительно в случае компрометации.

Компрометация ключа ЭП (Компрометация) – факт несанкционированного доступа или подозрение на несанкционированный доступ к носителю ключевой информации (Ключу ЭП). К событиям, связанным с компрометацией относятся, включая, но не ограничиваясь:

- утрата носителя ключевой информации, в том числе с последующим его обнаружением;
- увольнение сотрудника, имевшего доступ к носителю ключевой информации;
- утрата ключей от сейфа (нарушение целостности печати на сейфе, если используется процедура опечатывания сейфа) в момент нахождения в нем носителя ключевой информации;
- доступ посторонних лиц к носителю ключевой информации;
- несанкционированный удаленный доступ к носителю ключевой информации;
- иные обстоятельства, когда нельзя достоверно установить, что произошло с носителем ключевой информации, и прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа;

Корректная ЭП – ЭП электронного документа, дающая положительный результат её проверки с помощью Ключа проверки ЭП;

Криптографическая защита – защита Электронного документа от несанкционированного изменения и доступа к его содержимому посторонних лиц при помощи алгоритмов криптографического преобразования. В рамках Системы под криптографической защитой понимается шифрование, электронная подпись и вычисление хэш-функций программного обеспечения;

Логин – последовательность символов, являющаяся идентификатором Клиента в Системе;

Носитель ключевой информации (носитель ключа ЭП, eToken, USB-токен) – отчуждаемое (извлекаемое из компьютера) персональное средство аутентификации и защищенного хранения данных, исключающее возможность просмотра, изменения, копирования и печати содержимого. Использование USB-токенов является обязательным условием при работе в Системе в рамках Договора;

Пароль – известная только Клиенту последовательность символов, используемая Клиентом совместно с Логином для получения доступа к Системе;

Подлинность ЭД – положительный результат проверки ЭП, позволяющий установить авторство и факт неизменности содержания ЭД, включая все его реквизиты;

Программное обеспечение (ПО) – комплекс программ, обеспечивающий обработку и передачу данных, предназначенных для многократного использования и применения Сторонами;

Регламент УЦ – документ, являющийся неотъемлемой частью настоящих Правил и определяющий механизмы и условия предоставления и правила пользования услугами Удостоверяющего центра и основные организационно-технические мероприятия, необходимые для обеспечения работы УЦ и пользователей его услуг. Присоединение к настоящим Правилам автоматически означает присоединение к Регламенту УЦ;

Сертификат ключа проверки ЭП (сертификат) – Электронный документ или документ на бумажном носителе, выданный УЦ и подтверждающий принадлежность Ключа проверки ЭП владельцу Сертификата Ключа проверки ЭП;

Система дистанционного банковского обслуживания «МТИ-Банк» (АО) для юридических лиц и индивидуальных предпринимателей (Система ДБО, Система) – корпоративная система дистанционного банковского обслуживания BS-Client x64 Банка, включающая программно-аппаратный комплекс, состоящий из средств формирования, обработки, хранения и передачи электронных документов, а также средств электронной подписи, позволяющая Сторонам осуществлять защищенный обмен Электронными документами посредством сети Интернет. Система не имеет локальной базы данных Клиента на АРМ Клиента, доступ к базе данных Системы на сервере Банка осуществляется непосредственно с АРМ Клиента;

Система Антифрод (фрод-мониторинг) – установленная в Банке интеллектуальная система, предназначенная для оценки финансовых транзакций на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке;

Согласительная комиссия – комиссия, создаваемая для разрешения разногласий и споров между Клиентом и Банком при исполнении Договора об электронных расчетах;

Средство доверенного отображения подписываемых данных (SafeTouch) – подключаемое к USB-разъему компьютера Клиента устройство SafeTouch, в которое вставляется USB-токен. Позволяет вывести на свой экран данные подписываемого и передаваемого в Банк ЭПД и подтвердить подписание ЭПД нажатием соответствующей кнопки, что позволяет избежать подмены ЭПД с помощью вредоносного ПО или перехвата управления компьютером Клиента со стороны злоумышленников.

На экране устройства отображаются ИНН получателя платежа, БИК банка получателя, номер счета получателя и сумма платежа;

Средства ЭП – средства криптографической защиты информации (СКЗИ), используемые для создания ЭП, проверки ЭП, создания ключа ЭП и ключа проверки ЭП. В системе используется СКЗИ «КриптоПро CSP» (разработчик ООО «КРИПТО-ПРО»), соответствующее ГОСТ Р 34.10-2012 и требованиям нормативных актов Российской Федерации;

Стороны – Банк и Клиент;

Счет – расчетный или транзитный валютный счет Клиента, открытый в Банке;

Тарифы – Перечень тарифов за оказываемые Банком услуги по расчетно-кассовому обслуживанию юридических лиц, установленный Банком;

Удостоверяющий Центр (УЦ) - подразделение Банка, осуществляющее функции по созданию, выдаче и обслуживанию сертификатов ключей проверки Электронных подписей, а также иные функции, предусмотренные Регламентом УЦ и Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Хэш-функция – определенный математический способ проверки целостности ЭД, результат которого изображается в виде последовательности шестнадцатеричных цифр. Реализованный в Системе алгоритм вычисления хэш-функции соответствует стандарту ГОСТ Р 34.11-20012;

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, которая используется для определения лица, подписавшего информацию (усиленная неквалифицированная электронная подпись);

Электронный документ (ЭД) – документ в электронной форме, формируемый в формате Системы и/или посредством вложения файла формата Microsoft Word, Microsoft Excel или файла, содержащего графический экземпляр документа, подписанный (защищенный) ЭП, и имеющий равную юридическую силу с документом на бумажном носителе, подписанным собственноручными подписями уполномоченных лиц и заверенным оттиском печати;

Электронный платежный документ (ЭПД) – ЭД, подписанный одной или двумя ЭП, являющийся основанием для совершения операций по Счету Клиента.

2. КРАТКОЕ ОПИСАНИЕ СИСТЕМЫ ДБО

2.1. Система предназначена для предоставления Банком услуг по удалённому управлению Клиентом своими Счетами и обмена сопутствующей информацией посредством сети Интернет с использованием Электронных документов в соответствии с Документацией. Документация размещена на сайте Банка в сети Интернет по адресу http://www.mti-bank.ru/business/client-bank/enter. Клиент обязан руководствоваться Документацией, если настоящими Правилами не предусмотрено иное.

2.2. Для использования Системы Клиент должен иметь АРМ – компьютер (минимальные требования: процессор 1 ГГц, 2 Гбайт оперативной памяти, операционная система Microsoft Windows 7 и выше), подключённый к сети Интернет. В качестве браузера должен использоваться Microsoft Internet Explorer версии 8 и выше, Mozilla Firefox 4 (35) и выше, Google Chrome 6 (40) и выше.

2.3. Перед началом работы в Системе Клиенту необходимо:

- заключить Договор об электронных расчетах;
- определить необходимость использования дополнительного подтверждения (использование дополнительного подтверждения обязательно в случае, если не используется SafeTouch), допускается одновременное использование дополнительного подтверждения и SafeTouch. Дополнительное подтверждение может быть использовано только одним владельцем ЭП;
- предоставить номер мобильного телефона для получения SMS-сообщений (возможно использование только одного телефонного номера);
- получить в Банке необходимое количество носителей ключа ЭП, и получить необходимое количество устройств SafeTouch, если выбрано использование SafeTouch;
- получить в Банке Логин и временный пароль для регистрации в Системе;
- зарегистрироваться в Системе;
- сменить Пароль после первого входа в Систему;
- обеспечить создание ЭП, хранение Ключа ЭП на носителе Ключа ЭП;
- сформировать запрос на выпуск и регистрацию сертификата Ключа проверки ЭП в УЦ;
- сформировать с помощью Системы и распечатать 2 экземпляра Акта (далее также Акт) признания открытого ключа шифрования и Ключа проверки ЭП. Акт является документальным подтверждением запроса на выпуск и регистрацию Сертификата ключа проверки ЭП в УЦ. Клиент представляет в Банк два экземпляра указанного Акта на каждую ЭП, который принимается Банком с указанием даты его принятия. Акт должен быть подтвержден (заверен) подписью владельца ЭП, единоличного исполнительного органа и оттиском печати (при наличии) Клиента. После подписания Акта Банком один экземпляр передается Клиенту, а второй остается в Банке.
- получить от УЦ 2 экземпляра Сертификата на бумажном носителе, подписанные Банком, и предоставить в Банк подписанный со своей стороны экземпляр Сертификата. Данные Сертификата должны быть подтверждены (заверены) подписью единоличного исполнительного органа и оттиском печати (при наличии) Клиента. Один экземпляр Сертификата хранится у Клиента, а второй остается в Банке. Сертификат действует до истечения срока либо его отмены.

2.4. Клиент вправе предоставить право распоряжения денежными средствами на Счете с использованием Системы только лицам, указанным в предоставленной в Банк карточке с образцами подписей и оттиска печати Клиента, в соответствии с Заявлением о

сочетании подписей. Клиент обязан поддерживать соответствие между списком лиц, уполномоченных распоряжаться средствами на счете Клиента, указанных в карточке с образцами подписей и оттиска печати, с одной стороны, и владельцами ЭП (за исключением использования просмотровых ключей ЭП), с другой стороны. Банк не обязан отслеживать наличие такого соответствия.

2.5. Клиент самостоятельно принимает решение о количестве владельцев ЭП и порядке доступа к носителям Ключа ЭП.

2.6 Клиент вправе принять решение об использовании просмотрового Ключа ЭП.

2.7. Система позволяет Клиенту вводить, редактировать, удалять, подписывать и отправлять в Банк Электронные документы, перечисленные в п. 4.6 настоящих Правил, а также, по согласованию Сторон, просматривать информацию о состоянии своих Счетов в Банке и получать выписки по Счетам в электронном виде.

2.8. При обмене информацией для ее шифрования используется SSL-протокол.

2.9. Стороны признают, что:

- используемая Сторонами система защиты информации, обеспечивающая шифрование Электронных документов, формирование ЭП и контроль целостности ЭД, достаточна для защиты Системы от несанкционированного доступа, а также для подтверждения подлинности ЭД;
- Банк не гарантирует невозможность несанкционированного доступа к Системе третьими лицами, а Клиент принимает на себя соответствующие риски;
- если после заверения ЭД Электронной подписью этот ЭД был изменён, то эта ЭП становится некорректной, то есть её проверка даёт отрицательный результат;
- подделка ЭП, то есть создание корректной ЭП ЭД, направленного Клиентом, невозможна без использования ключа ЭП и пароля;
- ЭД, не подписанные ЭП или подписанные некорректной ЭП, не имеют юридической силы, не принимаются и не рассматриваются Банком.

2.10. Подлинниками ЭД являются:

2.10.1. Файл, который содержит текст этого ЭД и электронную подпись при условии положительного результата проверки корректности этой ЭП, произведённой программными средствами Системы с использованием Ключа проверки ЭП, зарегистрированной и принятой Банком в установленном порядке.

2.10.2. Бумажная распечатка этого ЭД, произведённая посредством Системы и заверенная собственноручными подписями уполномоченных лиц Стороны.

2.11. Ключ ЭП записывается Системой в зашифрованном виде на носитель ключа ЭП. Ключ ЭП должен храниться на носителе Ключа ЭП и используется владельцем ЭП в целях подписи ЭД, подготовленных с помощью Системы.

2.12. Ключ проверки ЭП после регистрации Клиента в Системе хранится Банком в базе данных Системы.

2.13. Архив входящих и исходящих документов в электронной форме хранится Банком в базе данных Системы.

2.14. Проверка корректности ЭП осуществляется в автоматическом режиме программными средствами Системы.

2.15. Для целей настоящих Правил Банк является владельцем Системы и по вопросам, прямо не урегулированным Правилами, вправе принимать решения по порядку функционирования Системы.

2.16. Все подключения к Системе, а также этапы обработки ЭД в Системе, фиксируются в электронных журналах Системы в автоматическом режиме. Стороны доверяют содержимому электронных журналов Системы.

3. УСЛОВИЯ ОРГАНИЗАЦИИ ОБМЕНА ЭД. ОСНОВАНИЯ ПРИОСТАНОВЛЕНИЯ ОБМЕНА ЭД

3.1. Стороны на условиях Договора об электронных расчетах осуществляют обмен ЭД, предусмотренными п. 4.6 настоящих Правил и подписанными (защищенными) ЭП, с использованием Системы.

3.2. Обмен ЭД осуществляется посредством направления документов, формируемых в шаблоне Системы ДБО, а также документов произвольного формата. Формирование Клиентом платежного поручения осуществляется как в шаблоне Системы, так и посредством импорта из бухгалтерской программы в формате, поддерживаемом Системой.

3.3. Проведение расчетных операций по Счетам Клиента осуществляется в соответствии с законодательством Российской Федерации, нормативными актами Банка России и договором банковского счета.

3.4. Стороны признают юридическую силу ЭД, подписанных (защищенных) ЭП (при установлении корректности ЭП), равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями законодательства Российской Федерации и с нормативными актами Банка России.

3.5 Для организации обмена ЭД Клиент выполняет следующие действия:

3.5.1. Самостоятельно и за свой счет комплектует АРМ необходимыми программно-техническими средствами в соответствии с п. 2.2 настоящих Правил.

3.5.2. Самостоятельно и за свой счет устанавливает отношения с организацией, обеспечивающей его доступ к Системе по телекоммуникационным каналам связи посредством сети Интернет.

3.5.3. Получает в Банке запечатанный конверт, содержащий Логин и временный пароль для доступа Клиента в Систему на бумажном носителе.

3.5.4. Получает в пользование в Банке носитель (носители) ключевой информации и, при необходимости, нужное количество устройств SafeTouch.

3.5.5. Обеспечивает создание владельцем ЭП Ключа ЭП, а также его сохранение на носитель Ключа ЭП.

3.5.6. Создаёт запрос в Системе на регистрацию сертификата Ключа проверки ЭП.

3.5.7. Формирует с помощью Системы и распечатывает 2 экземпляра Акта признания открытого ключа шифрования и Ключа проверки ЭП. Акт является документальным подтверждением запроса на выпуск и регистрацию Сертификата Ключа проверки ЭП в УЦ. Представляет в Банк два экземпляра указанного Акта на каждую ЭП, который принимается Банком с указанием даты его принятия. Акт должен быть подтвержден (заверен) подписью владельца ЭП, единоличного исполнительного органа и оттиском печати (при наличии) Клиента. После подписания Акта Банком, один экземпляр передается Клиенту, а второй остается в Банке.

3.5.8. Получает от УЦ 2 экземпляра Сертификата на бумажном носителе, подписанные Банком, и предоставляет в Банк подписанный со своей стороны экземпляр Сертификата. Данные сертификата должны быть подтверждены (заверены) подписью единоличного исполнительного органа и оттиском печати (при наличии) Клиента. Один экземпляр Сертификата остается у Клиента, а второй хранится в Банке. Сертификат действует до истечения срока либо до его отмены.

3.6. Для организации обмена ЭД Банк выполняет следующие действия:

3.6.1. Вносит сведения о Клиенте в Систему ДБО.

3.6.2. Обеспечивает реализацию функционала Системы по автоматическому формированию Логина и пароля для доступа Клиента в Систему, которые распечатываются на бумажном носителе и запечатываются в непрозрачный конверт.

3.6.3. Передает Клиенту запечатанный конверт, содержащий Логин и временный пароль для доступа Клиента в Систему ДБО на бумажном носителе, носитель (носители) ключевой информации и, при необходимости, Средство доверенного отображения подписываемых данных не позднее 5 (пяти) рабочих дней с даты открытия Счета в Банке или даты представления Клиентом Заявки на подключение к Системе ДБО (в зависимости от того, что наступит позднее).

3.6.4. В течение 2-х рабочих дней после получения от Клиента Акта признания открытого ключа шифрования и Ключа проверки ЭП, УЦ Банка формирует и выдает клиенту 2 экземпляра Сертификата ключа проверки ЭП Клиента на бумажном носителе, подписанные Банком.

3.6.5. После получения от Клиента подписанного экземпляра Сертификата, активирует Сертификат в УЦ. Сертификат действует до истечения срока либо его отмены.
3.6.6. Оказывает консультации по вопросам формирования и эксплуатации АРМ и Системы.
3.7. Стороны начинают осуществлять обмен ЭД с момента совершения действий, предусмотренных п.п. 3.5, 3.6.1 – 3.6.5 настоящих Правил.
3.8. Основаниями для приостановления Банком обмена ЭД являются:
3.8.1. Несоблюдение Клиентом требований к обмену ЭД и обеспечению информационной безопасности при обмене ЭД, предусмотренных нормативными актами Банка России и Договором об электронных расчетах.
3.8.2. Получение от Клиента уведомления о приостановлении обмена ЭД.
3.8.3. Компрометация Ключа ЭП. Обмен ЭД с Клиентом приостанавливается с момента получения Банком информации о компрометации Ключа ЭП.
3.8.4. Выход из строя или проведение регламентных работ в отношении программно-технических средств Системы или средств, обеспечивающих функционирование телекоммуникационных каналов связи.
3.8.5. Отсутствие возможности списания Банком денежных средств с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента для оплаты услуг Банка по Договору об электронных расчетах согласно п. 6 настоящих Правил.
3.8.6. Ограничение прав Клиента на осуществление операций по расчетным счетам Клиента в Банке в российских рублях.
3.8.7. Осуществление Клиентом деятельности, противоречащей законодательству Российской Федерации, нормативным актам Банка России, настоящим Правилам и договорам, заключенным с Банком.
3.8.8. Принятие Банком решения о приостановлении обмена ЭД по собственной инициативе.
3.9. Обмен ЭД возобновляется по решению Банка после устранения причин его приостановления.
3.10. Основаниями для прекращения обмена ЭД (одностороннего отказа Банка от Договора об электронных расчетах) являются:
3.10.1. Закрытие последнего Счета Клиента в Банке, распоряжение денежными средствами на котором осуществляется с использованием Системы ДБО. Договор об электронных расчетах прекращает свое действие с даты закрытия указанного Счета.
3.10.2. Получение от Клиента уведомления об отказе от пользования Системой ДБО.
3.10.3. Отсутствие возможности списания Банком денежных средств с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента для оплаты услуг Банка по Договору об электронных расчетах согласно п. 6 настоящих Правил.
3.10.4. Осуществление Клиентом деятельности, противоречащей законодательству Российской Федерации и нормативным актам Банка России.
3.10.5. Принятия Банком решения о прекращении обмена ЭД по собственной инициативе.
3.11. О приостановлении или о прекращении обмена ЭД (одностороннего отказа от Договора об электронных расчетах) Сторона-инициатор уведомляет другую Сторону письменно или направлением ЭД. Данный порядок не распространяется на п. 3.8.6, 3.10.1 настоящих Правил.

4. ОБЩИЕ ПРИНЦИПЫ ОБМЕНА ЭД

4.1. Стороны признают в качестве единой шкалы времени при направлении ЭД с использованием Системы Московское поясное время. Контрольным является время системных часов аппаратных средств Банка.
4.2. Стороны признают, что моментом поступления информации в Систему является текущее время по системным часам сервера Системы в момент полного помещения информации на жесткий магнитный диск сервера Системы.
4.3. Программно-технические средства Банка, обеспечивающие работоспособность Системы ДБО, функционируют в автоматическом режиме. Для входа в Систему ДБО Клиент должен ввести корректные Логин и пароль.
4.4. Обмен ЭД между Банком и Клиентом осуществляется с обязательным применением средств ЭП.
4.5. Статус ЭД, переданных в Банк, отслеживается АРМ автоматически при проведении Клиентом сеансов связи. Получение Клиентом ЭД из Банка осуществляется АРМ автоматически при проведении Клиентом сеансов связи.

Информирование Клиента о совершении обмена ЭД осуществляется направлением Клиенту соответствующего уведомления путем изменения статуса ЭД в Системе ДБО. Получение уведомлений производится путем ежедневного проведения Клиентом сеансов связи.

В случае не проведения или ненадлежащего проведения Клиентом сеансов связи, в том числе окончания сеанса связи до присвоения ЭД, переданному в Банк, статуса «принят», все связанные с этим негативные последствия возлагаются на Клиента.
4.6. Стороны используют следующие ЭД в формате Системы ДБО и в произвольном формате в соответствии с п. 3.1 настоящих Правил:
- ЭД Клиента: платежное поручение, платежное требование, инкассовое поручение, поручение на покупку иностранной валюты, поручение на продажу иностранной валюты, поручение на конверсию одной иностранной валюты в другую, поручение на перевод иностранной валюты, распоряжение на списание средств с транзитного валютного счета, справка о валютных операциях, запрос на получение выписки, запрос на отзыв ЭД, документ произвольного формата, документы, представляемые для осуществления валютных операций (паспорт сделки, обосновывающие и подтверждающие документы, справка о подтверждающих документах и т.п.), документы (копии документов), используемые в целях гражданско-правового оформления операций (договор, соглашение, контракт, оферта, акцепт, акт, письмо, претензия, запрос), иные документы по согласованию с Банком;
- ЭД Банка: выписка, приложение к выписке, документ произвольного формата.

4.7. Прием (отказ в приеме) ЭД подтверждается Банком, при этом происходит изменение статуса ЭД в Системе ДБО. Время приема (отказа в приеме) ЭД фиксируется в Системе ДБО.
4.8. Клиент имеет право отозвать составленный им и неисполненный Банком ЭПД, являющийся основанием для совершения операции по Счету Клиента в Банке, путем направления в Банк соответствующего ЭД.
4.9. Обмен ЭД между Банком и Клиентом осуществляется с использованием телекоммуникационных каналов связи; при невозможности их использования документооборот между Сторонами осуществляется в общем порядке на бумажных носителях.
4.10. В случае использования дополнительного подтверждения, после поступления в Банк ЭПД Клиента Система формирует SMS-сообщение, содержащее ИНН получателя платежа, БИК банка получателя, номер счета получателя, сумму платежа и код подтверждения. Для подтверждения корректности полученных Банком данных владелец ЭП вводит в Системе код подтверждения и ЭПД принимается Банком в обработку. В случае группового подтверждения переданных ЭПД, SMS-сообщение содержит только код подтверждения. При отсутствии кода подтверждения или вводе некорректного кода, ЭПД не считается доставленным и не принимается Банком в обработку.
4.11. Клиент полностью несет все риски, связанные с подключением АРМ к сети Интернет.
4.12. Стороны в рамках Договора об электронных расчетах вправе осуществлять обмен ЭД в соответствии с Инструкцией Банка России от 04.06.2012 № 138-И «О порядке представления резидентами и нерезидентами уполномоченным банкам документов и информации, связанных с проведением валютных операций, порядке оформления паспортов сделок, а также порядке учета уполномоченными банками валютных операций и контроля за их проведением».

5. ИСПОЛЬЗОВАНИЕ ЭП ПРИ ОБМЕНЕ ЭД

5.1. Стороны признают, что:

- используемые Сторонами в соответствии с Договором об электронных расчетах Система ДБО (логин и пароль), средства ЭП, которые реализуют подписание ЭП и шифрование ЭД, достаточны для обеспечения конфиденциальности, а также подтверждения подлинности и контроля целостности ЭД;
- внесение изменений в ЭД после его подписания ЭП дает отрицательный результат проверки ЭП;
- создание корректной ЭП возможно только с использованием ключа ЭП;
- по содержанию ЭД, подписанного ЭП, и ключа проверки ЭП невозможно определить ключ ЭП;
- каждая Сторона несет ответственность за сохранность своих Ключей ЭП, действия своих владельцев ЭП и своего персонала.

5.2. Для создания ЭП, подписания ЭД и проверки ЭП Стороны используют СКЗИ и признают ее достаточной для подтверждения подлинности ЭД.

5.3. Плановый срок действия Сертификата Ключа проверки ЭП определяется Банком и составляет 1 год. Плановая смена ключа ЭП производится владельцем ЭП и Клиентом самостоятельно. После даты окончания действия Сертификата Ключа проверки ЭП, ЭП не действует и, соответственно, передача документов через Систему не производится. О плановой замене Ключа ЭП Клиенту направляется уведомление с использованием Системы не позднее, чем за пять рабочих дней до окончания срока действия Сертификата Ключа проверки ЭП. В случае наступления даты окончания срока действия Сертификата Ключа проверки ЭП в нерабочий день, смена Ключа может быть проведена ранее срока истечения действия Сертификата Ключа проверки ЭП.

5.4. Внеплановая смена Ключей ЭП производится в случае их компрометации, а также в любое время по инициативе любой из Сторон в течение 5 (Пяти) рабочих дней с оплатой услуг Банка в соответствии с Тарифами. Внеплановая смена Ключей ЭП может производиться без оснований.

5.5. Для хранения носителей ключевой информации и конверта, содержащего Логин и пароль для доступа Клиента в Систему ДБО, должны использоваться металлические шкафы (сейфы), оборудованные надежными запирающими устройствами.

5.6. По окончании рабочего дня, а также вне времени составления и обмена ЭД, носители ключевой информации, конверт, содержащий Логин и пароль для доступа Клиента в Систему ДБО, должны храниться в металлических шкафах (сейфах).

5.7. Запрещается предпринимать попытки:
- копирования информации с носителя ключевой информации;
- ознакомиться с содержанием носителя ключевой информации;
- вывести Ключи ЭП на дисплей (монитор) компьютера или принтер;
- устанавливать носитель ключевой информации в компьютеры, не являющиеся АРМ;
- записать на носитель ключевой информации постороннюю информацию.

5.8. В случае принятия решения о компрометации ключа ЭП Клиент обязан любым доступным способом сообщить Банку о факте компрометации и прекратить использование скомпрометированных Ключей.

5.9. Стороны устанавливают, что:
- количество ЭП, используемых Клиентом для подписания одного ЭД, указывается в Заявке Клиента установленной Банком формы;
- количество владельцев ЭП определяется Клиентом самостоятельно в Заявке Клиента установленной Банком формы. В случае замены владельца ЭП, Клиент обязан письменно уведомить об этом Банк с предоставлением документов, подтверждающих полномочия владельца ЭП;
- в случае использования двух ЭП для подписания одного ЭД, ЭД признается подлинным только при положительном результате проверки обеих ЭП.

5.10. Банк имеет право производить замену средств ЭП и других средств, используемых при обмене ЭД, о чем уведомляет Клиента не менее чем за 30 (Тридцать) календарных дней. Клиент, при необходимости, обязан в установленный Банком срок приобрести и установить необходимые средства.

6. УСЛОВИЯ ОПЛАТЫ

6.1. Стоимость услуг, оказываемых Клиенту в соответствии с Договором об электронных расчетах, устанавливается Тарифами, действующими на день списания платы.

6.2. Оплата за носитель ключевой информации и\или устройство SafeTouch производится Клиентом не позднее даты его получения в Банке.

6.3. Оплата за обслуживание производится Клиентом за календарный квартал не позднее 25 числа месяца, предшествующего оплачиваемому календарному кварталу.

Оплата за обслуживание за календарный квартал, в котором заключен Договор об электронных расчетах, производится Клиентом не позднее даты получения Клиентом конверта с Логином и паролем. Оплата за обслуживание за календарный квартал, в котором заключен Договор об электронных расчетах, производится Клиентом пропорционально количеству полных месяцев текущего календарного квартала, начиная с даты получения Клиентом конверта с Логином и паролем.

6.4. При прекращении Договора об электронных расчетах возврат оплаты не производится.

6.5. Оплата услуг осуществляется Клиентом самостоятельно. Банк вправе списывать денежные средства в оплату стоимости услуг с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента на основании банковского ордера или инкассового поручения Банка. В случае отсутствия возможности списания Банком достаточной суммы с расчетного счета Клиента в Банке без дополнительного распоряжения Клиента, Клиент обязан незамедлительно принять меры по полному и своевременному получению Банком денежных средств, достаточных для оплаты услуг Банка.

7. ПРАВА И ОБЯЗАННОСТИ БАНКА

7.1. Банк вправе:

7.1.1. Консультировать Клиента по вопросам осуществления обмена ЭД.

7.1.2. Отказывать Клиенту в приеме ЭД с указанием причины отказа.

7.1.3. Отказать в регистрации сертификатов в случае невыполнения Клиентом условий, предусмотренных Договором об электронных расчетах.

7.1.4. Приостанавливать обмен ЭД при наличии оснований, предусмотренных п. 3.8 настоящих Правил.

7.1.5. Прекратить обмен ЭД (отказаться от Договора об электронных расчетах) при наличии оснований, предусмотренных п. 3.10 настоящих Правил.

7.1.6. Запрашивать у Клиента, при необходимости, копии ЭД на бумажном носителе.

7.1.7. Запрашивать у Клиента подтверждение или разъяснение совершаемых операций, а также в одностороннем порядке:
- установить для Клиента необходимость подтверждения исполнения ЭПД;
- ограничить общую сумму или количество неподтвержденных ЭПД.

Подтверждение или разъяснение запрашивается Банком у Клиента с использованием Системы либо иным образом. В этом случае ЭПД исполняется Банком только после получения требуемого подтверждения или разъяснения. Срок предоставления подтверждений и разъяснений устанавливается Банком.

7.1.8. В одностороннем порядке досрочно прекратить действие Ключа ЭП Клиента с последующим уведомлением об этом Клиента и потребовать от Клиента смены ключей ЭП. При этом обслуживание Клиента через Систему приостанавливается. Возобновление передачи ЭД с использованием Системы после её приостановления по инициативе Клиента или в связи с нарушением Клиентом

условий Настоящих Правил возможно только после устранения причин, которые были основанием такой приостановки работы с использованием Системы и получения Банком от Клиента заявления в письменной форме о возобновлении передачи ЭД с использованием Системы, при наличии у Банка возможности.
7.1.9. В одностороннем порядке вносить изменения в Правила, Документацию и Тарифы. Информация об этом размещается на информационных стендах Банка и/или на сайте Банка в сети Интернет не позднее чем за 10 (Десять) календарных дней до вступления изменений в силу.
7.1.10. Привлекать к работе по устранению недостатков Системы (если таковые будут установлены) её разработчика. Разработчик может привлекаться также при возникновении спорных ситуаций, связанных с использованием Системы, и к работе в Согласительной комиссии.
7.2. Банк обязан:
7.2.1. Исполнять поступившие от Клиента заверенные корректной ЭП ЭПД, оформленные в соответствии с законодательством и иными нормативными актами Российской Федерации, условиями заключенных между Банком и Клиентом договора банковского счета и Договора об электронных расчетах.
7.2.2. При получении от Клиента ЭД проверить корректность ЭП Электронного документа. При неудовлетворительном результате проверки ЭП отказать в проведении операции и/или приёме документа, при этом в Системе формируется сообщение о принятом решении.
7.2.3. После успешной проверки корректности ЭП провести первоначальный контроль правильности заполнения ЭД, проверить законность операции Клиента, соответствие договору банковского счета и Договору об электронных расчетах. Результатом этой работы является решение Банка о приёме или отказе в приеме ЭД Клиента.
7.2.4. Вести архивы входящих и исходящих ЭД в соответствии со следующими требованиями:
- входящие ЭД, прошедшие проверку корректности ЭП, хранятся с указанием даты и времени получения;
- все исходящие ЭД хранятся с указанием даты и времени их отправки;
- сроки хранения ЭД должны соответствовать срокам хранения, установленным для расчетных документов на бумажных носителях;
- порядок хранения ЭД должен обеспечивать оперативный доступ к ЭД и возможность распечатки их копий на бумажном носителе.

7.2.5. Обеспечивать своевременную смену ключей ЭП.
7.2.6. Незамедлительно информировать Клиента обо всех случаях возникновения технических неисправностей или других обстоятельствах, препятствующих обмену ЭД.
7.2.7. Осуществлять контроль ЭД, полученных от Клиента, и сообщать Клиенту об обнаруженных ошибках и причинах невозможности исполнения ЭД.
7.2.8. При получении от Клиента документа, извещающего о неуспешной выверке согласно п. 8.2.7. настоящих Правил, активизировать процедуры проверки, в том числе производить контроль входящих и исходящих ЭД, устанавливать причину расхождения и, при обнаружении ошибок со своей стороны, передавать Клиенту исправленные документы.
7.2.9. Изготавливать, при необходимости, бумажные копии ЭД.
7.2.10. Предоставлять Клиенту по его запросу бумажные копии ЭД.
7.2.11. Консультировать Клиента по вопросам осуществления обмена ЭД.
7.2.12. Исключить доступ неуполномоченных лиц к Системе, средствам ЭП, Ключам ЭП и Ключам проверки ЭП.
7.2.13. В случае выявления системой Антифрод подозрительного платежа, связаться с Клиентом для подтверждения данного платежа. При невозможности связаться с Клиентом Банк вправе не проводить такой платёж до подтверждения его Клиентом.

8. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА

8.1. Клиент вправе:
8.1.1. Использовать ПО в соответствии с положениями Договора об электронных расчетах и Документацией.
8.1.2. Обращаться в Банк с запросами по вопросам обмена ЭД и функционирования АРМ.
8.1.3. Обращаться в Банк с заявлением о предоставлении копий ЭД, хранимых Банком.
8.1.4. Самостоятельно распоряжаться денежными средствами, находящимися на его Счетах, в порядке и пределах, установленных законодательством и иными нормативными актами Российской Федерации.
8.1.5. Отозвать переданные в Банк с использованием Системы ЭД, которые ещё не исполнены Банком. При этом Клиент может использовать информационные сообщения и письма, предусмотренные в Системе.
8.1.6. Получать в Банке консультации по обслуживанию с использованием Системы.
8.1.7. В случае возникновения у Клиента технических неисправностей или других обстоятельств, препятствующих использованию ЭД, а также в других случаях, установленных Правилами, обратиться в Банк с письменной просьбой об отмене или приостановлении обслуживания с использованием Системы.
8.2. Клиент обязан:
8.2.1. Строго соблюдать Договор об электронных расчетах и Документацию.
8.2.2. Передавать в Банк ЭД и просматривать (получать) информацию из Банка с использованием Системы только с исправного компьютера, в котором отсутствуют компьютерные вирусы и программы, направленные на разрушение, модификацию Системы или изменение её функциональных свойств.
8.2.3. Соблюдать порядок обмена ЭД, а также обеспечивать сохранность, целостность и работоспособность АРМ в соответствии с Требованиями, указанными в п. 12 настоящих Правил. В целях повышения безопасности Клиенту рекомендуется использовать Средство достоверного отображения подписываемых данных, а также подтверждать ЭПД по отдельности.
8.2.4. Своевременно информировать Банк о технических неисправностях или других обстоятельствах, препятствующих обмену ЭД, и по запросу Банка предоставлять письменное разъяснение таких обстоятельств.
8.2.5. Соблюдать лицензионные ограничения разработчиков Системы и средств ЭП, использовать ПО и АРМ только в целях, установленных Договором об электронных расчетах.
8.2.6. Использовать при обмене только соответствующие установленному перечню ЭД.
8.2.7. Осуществлять контроль полученных от Банка ЭД и при обнаружении ошибок незамедлительно информировать о них Банк письменно или направлением ЭД.
8.2.8. Ежедневно по рабочим дням проводить сеансы связи. Инициатором связи с Банком с использованием Системы всегда выступает Клиент. Любая просрочка в выполнении Банком своей обязанности, которая произошла из-за отсутствия инициативы Клиента в установлении связи с Банком с использованием Системы, не влечёт за собой ответственности Банка.
8.2.9. Проводить выверку путем проверки соответствия реквизитов ЭД, являющихся основанием для совершения операций по счетам Клиента в Банке, реквизитам выписки. В случае установления расхождений не позднее следующего банковского дня с даты совершения операции письменно или направлением ЭД извещать Банк об отрицательных результатах выверки с указанием перечня не прошедших контроль реквизитов. Неполучение Банком от Клиента извещения об отрицательных результатах выверки в указанный срок является подтверждением правильности исполнения ЭД.
8.2.10. Не пытаться вносить никаких изменений в Систему.
8.2.11. Обеспечить сохранность АРМ, ключей ЭП и защиту носителей ключевой информации, Логина и пароля для доступа Клиента в Систему ДБО, от несанкционированного доступа. Не сообщать посторонним лицам Кодовое слово. Носитель ключевой информации, Сертификат Ключа проверки ЭП, Логин и пароль должны храниться исключительно у владельца ЭП и ни при каких обстоятельствах не

должны передаваться или раскрываться неуполномоченным лицам. Ответственность за использование АРМ, Логина и пароля, носителя ключевой информации и Ключей ЭП вне зависимости от обстоятельств полностью несёт Клиент.
8.2.12. Менять ключи ЭП не реже одного раза в год, либо по указанию Банка; каждый раз при изменении состава лиц, уполномоченных распоряжаться Счётом Клиента, прекращать действие Ключей ЭП лиц, чьи полномочия на распоряжение средствами по Счету прекращены и предоставлять Ключи проверки ЭП на вновь уполномоченных лиц в порядке, изложенном в п.п. 3.5.5 – 3.5.8 настоящих Правил.
8.2.13. Незамедлительно уведомлять Банк о компрометации ключа ЭП, а также сообщать Банку о всех ошибках при совершении переводов средств и о несанкционированных переводах средств в письменном виде после их обнаружения немедленно (в день обнаружения). При обращении в Банк с сообщением о компрометации по телефону, Клиент использует Кодовое слово.

Под ошибкой понимается, но не ограничивается этим:

- неверный перевод средств со счёта Клиента;
- ошибка в компьютерных или бумажных расчётах, выполняемых Банком в связи с переводом средств;
- неправильное указание суммы перевода или получателя платежа в выписке по счёту Клиента.

Под несанкционированным переводом средств понимается, но не ограничивается этим, перевод средств со счёта Клиента, произведённый лицами, не имеющими права распоряжаться Счетами Клиента. Это включает в себя любой перевод средств, если он:

- совершен любым лицом, которому носитель ключевой информации не принадлежит на законном основании;
- совершен без поручения Клиента и при отсутствии законных оснований для этого.

8.2.14. По требованию Банка в течение 3 (Трех) дней передавать Банку письменное изложение обстоятельств, связанных с отправкой документов, ЭП которых не была признана Банком корректной, и со всеми случаями ошибок и несанкционированных переводов средств или таких попыток, а также все относящиеся к таким случаям документы и файлы с информацией.
8.2.15. Немедленно сообщать Банку в письменном виде обо всех случаях, свидетельствующих о попытках неуполномоченных лиц получить доступ к Счетам Клиента с использованием Системы, а также о любой потере контроля над носителем Ключа ЭП и/или Сертификатом. При выявлении указанных выше фактов и другой компрометации или подозрении на компрометацию своего Ключа ЭП Клиент обязан немедленно поменять Ключи ЭП. Новые Ключи проверки ЭП регистрируются и передаются в Банк в соответствии с п.п. 3.5.5 –3.5.8 настоящих Правил.
8.2.16. По запросу Банка предоставлять копии ЭД на бумажном носителе в течение 3 (Трех) рабочих дней с даты получения запроса.
8.2.17. В срок, указанный Банком, предоставлять Банку подтверждение проводимой операции согласно п. 7.1.7 настоящих Правил.
8.2.18. Предоставлять представителям Согласительной комиссии доступ в помещение, где установлен компьютер, с которого производилась передача спорного документа, а также к самому компьютеру для проведения проверок соблюдения Клиентом Договора об электронных расчетах и Документации.
8.2.19. Своевременно производить оплату услуг Банка.
8.2.20. Представить Заявку установленной Банком формы при необходимости внесения изменений в перечень Счетов, распоряжение денежными средствами, на которых может осуществляться с использованием Системы ДБО.
8.2.21. Предоставить в Банк при наступлении события, указанного в п. 8.2.13 настоящих Правил, а также в случае выявления осуществлённой или предотвращенной попытки списания денежных средств со Счета Клиента с использованием Системы (при наличии соответствующей возможности):

- энергонезависимые технические данные, расположенные на запоминающих устройствах средств вычислительной техники (далее СВТ), используемых клиентом для осуществления доступа к Системе:
  - серверном оборудовании;
  - настольных компьютерах, ноутбуках;
  - мобильных устройствах и планшетах;
- энергозависимые технические данные, расположенные в оперативной памяти СВТ, используемых клиентом для осуществления доступа к Системе;
- энергозависимые технические данные операционных систем СВТ, используемых клиентом для осуществления доступа к Системе:
- данные о сетевых конфигурациях;
- данные о сетевых соединениях;
- данные о запущенных программных процессах;
- данные об открытых файлах;
- список открытых сессий доступа;
- системные дату и время операционной системы;
- протоколы (журналы) регистрации телекоммуникационного оборудования, используемого клиентами для осуществления доступа к Системе:
- маршрутизаторы, коммутаторы, точки и контроллеры беспроводного доступа, модемы;
- DHCP-сервисы;
- протоколы (журналы) регистрации средств защиты информации;
- средства (системы) аутентификации, авторизации и разграничения доступа к Системе;
- средства зашиты от несанкционированного доступа, размещенные на СВТ, используемых клиентом для осуществления доступа к Системе;
- средства межсетевого экранирования;
- средства обнаружения вторжений и сетевых атак;
- средства антивирусной защиты;
- средства криптографической защиты информации, используемые в системе ДБО;
- протоколы (журналы) регистрации и данные почтовых серверов и средств контентной фильтрации электронной почты;
- данные сетевого трафика из (в) сегмента (сегмент) вычислительной сети, в котором расположены СВТ, используемые клиентом для осуществления доступа к Системе;
- протоколы (журналы) регистрации автоматических телефонных станций;
- протоколы (журналы) регистрации и данные систем видеонаблюдения и систем контроля доступа, используемые для контроля доступа в помещения, в которых расположены СВТ, используемые клиентом для осуществления доступа к Системе;
- носители ключевой информации СКЗИ, используемой в Системе.

9. ОТВЕТСТВЕННОСТЬ СТОРОН

9.1. За неисполнение или ненадлежащее исполнение своих обязательств, принятых на себя в рамках настоящих Правил, Стороны несут ответственность в соответствии с действующим законодательством РФ.
9.2. Клиент несёт ответственность за содержание любого ЭД, подписанного его ЭП, вне зависимости от того, кто подписал документ - лицо уполномоченное, распоряжаться Счетом, или нет. Банк несет ответственность за содержание любого ЭД, подписанного его ЭП.
9.3. При несвоевременном сообщении в Банк об ошибках, о несанкционированных переводах средств, о случаях утраты или компрометации ключей ЭП, Сертификата ключа, раскрытия пароля, а также о других подобных обстоятельствах ответственность за связанные с этим убытки несёт Клиент. Все действия Банка, совершенные до получения от Клиента письменного уведомления о вышеуказанных случаях, считаются совершёнными Банком на законном основании и не влекут ответственности Банка.

9.4. Клиент несет полную ответственность за все убытки, которые могут возникнуть у него или у Банка в результате неправильного перевода Банком средств Клиента из-за нарушения Клиентом условий Договора или Правил (вне зависимости от причин нарушения условий Договора или Правил). В этом случае Банк освобождается от возмещения убытков Клиенту.
9.5. Банк не несёт никакой ответственности в случае причинения Клиенту убытков исполнением ЭД, подписанных корректной ЭП, в результате передачи этих документов с использованием Системы неуполномоченными на то лицами, включая использование пароля, Сертификата Ключа проверки ЭП и Ключей ЭП Клиента (вне зависимости от причин получения неуполномоченными лицами доступа к Ключам ЭП, информации о паролях, в том числе при их утере, добровольной передаче Клиентом неуполномоченным лицам, краже, грабеже, разбое и других обстоятельствах их передачи неуполномоченным лицам). В этом случае убытки Клиента образуются по вине Клиента и возмещению со стороны Банка не подлежат.
9.6. В случае несвоевременного приостановления Банком обмена ЭД с использованием Системы после получения письменного сообщения Клиента о хищении носителей Ключа ЭП, попытках совершения несанкционированных переводов средств Клиента и иных подобных сообщений Банк возмещает Клиенту причинённые этим убытки.
9.7. Убытки, образовавшиеся в связи с неисполнением или ненадлежащим исполнением Банком ЭД Клиента по причине наличия вирусов в компьютерном обеспечении одной из Сторон, ложатся на эту Сторону и другой Стороной не возмещаются. Убытки также не возмещаются Сторонами при одновременном наличии вирусов в компьютерном обеспечении двух Сторон.
9.8. Клиент самостоятельно несет ответственность за возможные убытки, возникшие в связи с передачей ЭД и получением информации с использованием Системы.
9.9. Стороны не несут ответственности за работу сети Интернет, ее программ и протоколов, а также иных телекоммуникационных каналов и систем связи, включая проводную и мобильную телефонную связь. Убытки, возникшие у одной из Сторон при их полной или частичной неработоспособности, другой Стороной не возмещаются.
Никакие претензии по работоспособности сети Интернет, ее программ и протоколов, иных телекоммуникационных каналов и систем Сторонами не принимаются и не рассматриваются.
9.10. Клиент согласен с тем, что Банк не несёт никакой ответственности за ошибки или сбои в работе Системы, если они произошли не по вине Банка (в том числе по вине разработчика Системы), даже если они повлекли убытки Клиента. Указанные убытки Банком не возмещаются.
9.11. Стороны освобождаются от ответственности в том случае, если используемые в Системе алгоритмы не соответствуют ГОСТам, указанным в технической документации к Системе и Правилах, а также при нарушении разработчиком установленных правил изготовления (разработки) Системы. Возникшие в связи с этим убытки Сторонами не возмещаются.
9.12. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если это явилось следствием действия обстоятельств непреодолимой силы (форс-мажорные обстоятельства). В этом случае срок исполнения обязательств отодвигается соразмерно времени действия таких обстоятельств.
Понятие форс-мажорных обстоятельств охватывает внешние или чрезвычайные события, отсутствовавшие во время заключения Договора об электронных расчетах и возникшие помимо воли и желания Сторон; наступление этих событий Стороны не могли предотвратить разумными мерами и средствами, которые было бы оправдано ожидать от Стороны в конкретной ситуации, пострадавшей от воздействия форс-мажорных обстоятельств. К форс-мажорным обстоятельствам Стороны также относят следующее: отключение и/или перебои электроэнергии; наличие вирусов в сети Интернет; действия Центрального Банка РФ и иных органов власти, влияющие на осуществление платежей и/или использование Системы; принятие законодательных актов, изменяющих или отменяющих порядок осуществления платежей с использованием Электронных документов; вооруженные конфликты; стихийные бедствия; пожары; взрывы; отказы компьютерных систем; отказы или ненадлежащее функционирование телекоммуникационных линий связи, если указанные обстоятельства непосредственно повлияли на исполнение Сторонами своих обязательств.
Сторона, подвергшаяся воздействию форс-мажорных обстоятельств, должна незамедлительно, не позднее 5 (Пяти) рабочих дней, известить в письменной форме другую Сторону о типе, характере, возможной продолжительности и предположительных последствиях действия данных обстоятельств, а также принять все возможные меры с целью максимально ограничить отрицательные последствия, вызванные указанными обстоятельствами. Сторона, для которой создались форс-мажорные обстоятельства, должна также не позднее чем через 5 (Пять) рабочих дней известить в письменной форме другую Сторону о прекращении этих обстоятельств. В этом случае ни одна из Сторон не будет иметь права на возмещение другой Стороной любых возможных убытков.
Неизвещение или несвоевременное извещение Стороной, для которой создалась невозможность исполнения обязательств по Договору, о наступлении форс-мажорных обстоятельств другой Стороны, влечет за собой утрату права ссылаться на эти обстоятельства.
9.13. За неисполнение или ненадлежащее исполнение своих обязательств по Договору Банк несёт ответственность перед Клиентом только при наличии своей вины.
9.14. В связи с тем, что Клиент в любом случае имеет возможность представлять в Банк расчётные документы на бумажном носителе, Банк не несёт ответственность перед Клиентом за несвоевременное представление Клиентом документов в Банк при невозможности передачи ЭД с использованием Системы, в том числе при её неработоспособности или приостановлении обслуживания.
9.15. Клиент несет всю ответственность за использование Системы при изменении списка лиц, имеющих право распоряжаться денежными средствами Клиента, до момента представления в Банк новой карточки с образцами подписей и оттиска печати и заявки на смену Ключей ЭП установленной Банком формы.
Банк имеет право приостановить работу с использованием Системы ДБО до даты предоставления всех необходимых документов, требуемых Банком. Стороны признают, что все ЭД, направленные Клиентом в Банк с использованием Системы ДБО, принятые, успешно расшифрованные и исполненные Банком, считаются до момента внесения соответствующих изменений в Договор надлежащим образом оформленными и исполненными в соответствии с Договором.
9.16. Банк не несет ответственности за ЭД Клиента, проведенные по старым реквизитам, в случае несвоевременного непредставления Клиентом информации о произошедших изменениях и направления в Банк документально подтвержденных новых реквизитов.
9.17. Клиент несет ответственность за сохранность полученных в Банке носителей ключевой информации и средств доверенного отображения подписываемых данных. В случае выхода из строя носителя ключевой информации или средства доверенного отображения подписываемых данных, находящегося у Клиента менее 6 месяцев и не имеющего физических повреждений, Банк производит его замену бесплатно. Во всех остальных случаях Клиент оплачивает замену в соответствии с Тарифами.

10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

10.1. Споры, возникающие при исполнении Договора об электронных расчетах, разрешаются Сторонами путем переговоров.
В случае возникновения у Сторон споров по поводу приема (отказа в приеме) ЭД, они регулируются следующим образом (досудебный порядок урегулирования споров):
- в течение 5 (Пяти) календарных дней с момента возникновении разногласий Сторонами создается Согласительная комиссия, в состав которой включаются по 2 (Два) представителя от каждой из Сторон и эксперт (представитель обладателя исключительных прав на ПО Системы ДБО) при необходимости могут быть приглашены представители разработчиков Системы, СКЗИ и устройств, используемых для работы в Системе;

➢ Согласительная комиссия проверяет идентичность Ключа проверки ЭП Клиента, которым подписан спорный ЭД, а также осуществляет проверку правомерности приема (отказа в приеме) ЭД с учетом положений Документации и условий функционирования Системы ДБО;
➢ по результатам работы Согласительной комиссией простым большинством голосов принимается решение, которое оформляется соответствующим актом, подписываемым экспертом; Стороны признают данный акт надлежащим и окончательным документом, разрешающим возникшие разногласия.
10.2. Клиент возмещает Банку расходы, связанные с оплатой услуг эксперта, в случае признания претензий Клиента в отношении Банка необоснованными, при этом оплата производится согласно п. 6 Договора об электронных расчетах.
10.3. Все разногласия, споры и конфликтные ситуации, возникающие между Сторонами вследствие исполнения Договора, разрешаются с учетом взаимных интересов путем переговоров. На время разрешения спорной ситуации Банк имеет право немедленно приостановить обмен ЭД в одностороннем порядке с соответствующим уведомлением Клиента.
10.4. В случае не урегулирования спора Сторонами он передается на рассмотрение Арбитражного суда г. Москвы.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Договор об электронных расчетах является неотъемлемой частью Договора банковского счета, заключенного между Банком и Клиентом.
11.2. Допускается заключение и расторжение Договора об электронных расчетах посредством направления в Банк документов в электронном виде, подписанных согласованной Сторонами ЭП в порядке, предусмотренном соглашением сторон.
11.3. Сформированные до вступления в силу настоящей редакции Правил Ключи ЭП продолжают действовать до их замены в порядке, установленном настоящими Правилами.
11.4. Любая из Сторон вправе расторгнуть Договор в одностороннем (внесудебном) порядке, предупредив об этом другую Сторону письменно не менее чем за 10 (Десять) календарных дней до предполагаемой даты расторжения Договора. До даты расторжения Договора Клиент обязан оплатить задолженность перед Банком, возникшую вследствие исполнения Договора.
11.5. Заявки, направляемые Клиентом в Банк в рамках Договора, оформляются по установленной Банком форме.
11.6. Настоящие Правила вступают в силу с даты их утверждения Банком.
11.7. По Договору об электронных расчетах, заключенному до указанной в п. 11.6 настоящих Правил даты, в целях перехода на новую версию Системы ДБО Клиент обязан предоставить в Банк Заявку на подключение к Системе ДБО и выполнить действия, предусмотренные в п. 3.5. настоящих Правил. При этом, для входа в Систему ДБО Клиент использует прежнюю ссылку на сайте Банка и сформированные до указанной в п. 11.6 настоящих Правил даты Ключи ЭП продолжают действовать (за исключением случая их компрометации) до активации Банком первого подписанного Клиентом Сертификата в соответствии с п. 3.6.5 настоящих Правил.

12. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ СКЗИ

12.1. Требования по организационному обеспечению безопасности СКЗИ:
➢ Клиент выделяет (определяет) лиц, ответственных за обеспечение безопасности информации и эксплуатации СКЗИ;
➢ Клиент разрабатывает внутренние документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ;
➢ к работе с СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.
12.2. Требования по размещению СКЗИ и режиму охраны:
➢ помещение, в котором размещается АРМ Клиента, должно обеспечивать конфиденциальность проводимых работ;
➢ помещение и его оборудование должны исключать возможность бесконтрольного проникновения в него посторонних лиц и обеспечивать сохранность находящихся в нем конфиденциальных документов и технических средств;
➢ размещение оборудования и технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
➢ входная дверь помещения должна быть оборудована замком, обеспечивающим надежное закрытие помещения в нерабочее время;
➢ размещение технических средств в помещении должно исключать возможность визуального просмотра конфиденциальных документов и экрана монитора, на котором они отражаются, другими лицами;
➢ системный блок компьютера с АРМ Клиента оборудуется средствами контроля вскрытия;
➢ ремонт и/или последующее использование системного блока осуществляется после удаления с него АРМ Клиента.
12.3. Требования по обеспечению безопасности ключевой информации:
➢ носители ключевой информации Клиент получает под поэкземплярный учет в выделенных для этих целей журналах;
➢ учет и хранение носителей ключевой информации поручается руководством Клиента специально выделенным сотрудникам;
➢ для хранения носителей ключевой информации выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
12.4. С целью исключения возможности хищения ключевой информации третьими лицами необходимо:
➢ использовать только лицензионное программное обеспечение;
➢ установить актуальное антивирусное программное обеспечение на АРМ Клиента и регулярно обновлять вирусные базы данных;
➢ исключить возможность разглашения ключевой информации;
➢ установить программное обеспечение, исключающее несанкционированное использование АРМ Клиента;
➢ при подозрении о компрометации Ключей ЭП незамедлительно обращаться в Банк с заявлением о компрометации Ключей ЭП.
12.5. Несоблюдение требований информационной безопасности может привести к хищению персональной, ключевой информации, использованию АРМ Клиента неуполномоченными лицами.
12.6. В случае несоблюдения требований информационной безопасности Клиентом, недостаточного внимания Клиента к применению программно-технических средств и к реализации организационных мер, направленных на соблюдение информационной безопасности, за несанкционированное списание денежных средств со счета Клиента Банк ответственности не несет.