

ПРАВИЛА ОБМЕНА
ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ПО СИСТЕМЕ
«КЛИЕНТ-БАНК» в ПАО «МТС-Банк»

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1.** Настоящие Правила обмена электронными документами по системе «Клиент-Банк» в ПАО «МТС-Банк» (далее – Правила) устанавливают порядок обслуживания Клиентов с использованием Системы «Клиент-Банк» (далее – Система «Клиент-Банк», Система) в целях предоставления услуг по Дистанционному банковскому обслуживанию и определяют возникающие в этой связи права, обязанности и ответственность Сторон.
- 1.2.** Правила являются типовым документом Банка и могут быть приняты Клиентом путем присоединения к Правилам в целом в порядке, установленном Правилами.
- 1.3.** Заключение Договора об обслуживании с использованием Системы «Клиент-Банк» (далее - Договор) осуществляется Клиентом в соответствии со статьей 428 Гражданского кодекса Российской Федерации путем предоставления в Банк ***Заявления о присоединении к Правилам обмена электронными документами по Системе «Клиент-Банк»*** на бумажном носителе, составленного по форме ***Приложения №1*** к настоящим Правилам с проставлением отметки о приеме уполномоченным сотрудником **Банка** на Заявлении. Для подключения Клиента к Системе «Клиент-Банк» одновременно с Заявлением о ***присоединении к Правилам обмена электронными документами по Системе «Клиент-Банк» в Банк*** представляются на бумажном носителе: Заявка на подключение к Электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» (Приложение № 7, № 7а (в зависимости от предоставленных прав подписи) к Правилам), Заявление на регистрацию в Удостоверяющем центре Банка (Приложение № 8 к Правилам), Заявка на установление ограничения на подключение к электронной системе «Клиент-Банк» по сетевым адресам (Приложение № 6 к Правилам), в случае если **Клиент** ограничения установил.
- 1.4.** Для идентификации Банком лиц-владельцев ключей электронной подписи (и шифрования), указанных в Заявке на подключение к Электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» (Приложение № 7, № 7а (в зависимости от предоставленных прав подписи) к Правилам), в Банк должны быть предоставлены документы, удостоверяющие личности (оригиналы или нотариально заверенные копии), и документы, подтверждающие полномочия указанных лиц на использование аналогов собственноручной подписи (электронной подписи) (оригиналы или заверенные в установленном порядке копии с предоставлением оригиналов для сверки) в случае не представления данных документов ранее для открытия/ведения банковских счетов.
- 1.5.** В случае, если между Клиентом и Банком ранее заключен Договор об обслуживании Клиента по электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации», Клиент подтверждает согласие (акцепт) на осуществление электронного документооборота на условиях настоящей редакции Правил путем представления в Банк ***Заявления о присоединении к Правилам обмена электронными документами по Системе «Клиент-Банк»*** на бумажном носителе, составленного по форме (***Приложения №1***) к настоящим Правилам с проставлением отметки о приеме уполномоченным сотрудником **Банка** на Заявлении.
- 1.6.** Банк с целью ознакомления Клиента с условиями Правил размещает Правила путем их опубликования в порядке, предусмотренном ***разделом 16*** Правил.
- 1.7.** Дистанционное банковское обслуживание Клиента с использованием Системы осуществляется в соответствии с законодательством Российской Федерации и Правилами. В
-

случае изменения законодательства Российской Федерации Правила, до момента их изменения Банком, применяются в части, не противоречащей требованиям законодательства Российской Федерации.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ

В целях настоящих Правил **Стороны** используют следующие термины:

2.1. Авторство документа – принадлежность документа одной из **Сторон** по Договору. Авторство электронного документа определяется принадлежностью электронной подписи конкретному пользователю Системы.

2.2. Администратор (Оператор) Удостоверяющего центра – должностное лицо, ответственное за решение комплекса задач по организации и обеспечению защиты информации с использованием СКЗИ, в том числе обеспечение функционирования СКЗИ **Клиентов** Системы.

2.3. Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

2.4. Аутентификация информации – установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и что она при этом не заменена и не искажена. Любые преднамеренные и случайные попытки искажений информации обнаруживаются с соответствующей вероятностью.

2.5. Безопасность информации (информационная безопасность):

- состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.;
- состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

2.6. Владелец сертификата ключа проверки электронной подписи – физическое лицо (ответственный сотрудник Банка или Клиента), на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи, и которое владеет соответствующим ключом ЭП, позволяющим с помощью средств ЭП создавать ЭП в электронных документах (подписывать электронные документы). Владельцами сертификатов ключей проверки ЭП являются уполномоченные лица Сторон, имеющие право подписывать электронные документы своей ЭП от имени Стороны.

2.7. Документ в электронной форме (электронный документ – ЭД) – документ, представленный в электронной форме в виде файла или записи базы данных, заверенный электронной подписью (ЭП) уполномоченного лица Клиента или Банка, подготовленный и переданный с помощью программного обеспечения Системы в соответствии со всеми процедурами защиты информации.. Электронный документ, содержащий распоряжение Клиента, должен соответствовать требованиям нормативных актов Банка России и внутренних нормативных актов Банка, определяющих порядок оформления распоряжений и выполнения процедур приема к исполнению и исполнения распоряжений.

2.8. Ключ ЭП (и шифрования) – (закрытый ключ) – уникальная последовательность символов, предназначенная для создания в электронных документах ЭП, а так же преобразования полученной закрытой информации в открытую с использованием сертифицированных средств криптографической защиты информации.

2.9. Защита информации – комплекс мероприятий, проводимых с целью предотвращения

утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации.

2.10. Компрометация закрытого ключа ЭП (и шифрования), пароля доступа к Системе – событие, в результате которого возникает возможность ознакомления неуполномоченных лиц с закрытым ключом ЭП (и шифрования), паролем доступа к Системе. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- Безвозвратная утрата носителей закрытого ключа;
- Утрата носителей закрытого ключа с последующим обнаружением;
- Увольнение работников, имевших доступ к носителям закрытого ключа и паролю для доступа к Системе;
- Нарушение правил хранения и уничтожения (после окончания срока действия) носителей закрытого ключа;
- Возникновение подозрений на утечку информации или её искажение в Системе;
- Нарушение печати на сейфе или пенале (контейнере) с носителями закрытого ключа;
- Случаи, когда невозможно достоверно установить, что произошло с носителями закрытого ключа, в том числе случаи, когда носители закрытого ключа вышли из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника.

2.11. Лицензия в области защиты информации – оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

2.12. Мероприятия по защите информации – совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

2.13. Обработка информации – передача, прием, хранение, преобразование и отображение информации.

2.14. Ключ проверки ЭП – (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи, а так же преобразования передаваемой открытой информации в закрытую.

2.15. Плановая смена ключей – смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей.

2.16. Подтверждение подлинности ЭП в электронном документе – положительный результат проверки средствами ЭП с использованием сертификата ключа подписи принадлежности ЭП в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной ЭП документе.

2.17. Проверка электронной подписи документа – проверка соотношения, связывающего хеш-функцию документа, подпись под этим документом и открытый ключ подписавшего абонента. Если рассматриваемое соотношение оказывается выполненным, то подпись признается правильной, а сам документ – подлинным, в противном случае документ считается измененным, а подпись под ним – недействительной.

2.18. Реестр Сертификатов – набор документов в электронной и/или бумажной форме, включающий следующую информацию:

- запросы на регистрацию в Удостоверяющем Центре;
- список пользователей Удостоверяющего Центра;
- запросы на изготовление сертификатов ключей подписи;
- запросы на аннулирование (отзыв) сертификатов ключей подписи;
- запросы на приостановление/возобновление действия сертификатов ключей подписи;
- сертификаты ключей подписи;
- списки отзыванных сертификатов.

2.19. Сертификат ключа проверки ЭП (сертификат ключа подписи) – документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица Удостоверяющего Центра, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.20. Система «Клиент-Банк» (Система) – системы дистанционного банковского обслуживания Традиционный «Клиент-Банк» и Интернет «Клиент-Банк» производства ООО «Банк Софт Системс» (Компания BSS), которые позволяют осуществлять формирование, передачу и хранение документов в электронном виде. Система «Клиент-Банк» предназначена для повышения качества обслуживания Клиента, а также для ускорения выполнения расчетных операций Клиента за счет замены бумажного документооборота между Банком и Клиентом на документооборот с использованием электронных документов, передаваемых для исполнения в Банк по каналам связи.

2.21. Средства ЭП – 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.

2.22. Удостоверяющий Центр – подразделение Банка, осуществляющее следующие функции:

- изготовление и выдачу сертификатов ключей подписей;
- создание (генерация) закрытых и открытых ключей;
- установление сроков действия сертификатов ключей подписей;
- приостановление и возобновление действия сертификатов ключей подписей, а также их аннулирование;
- ведение Реестра Сертификатов, обеспечение его актуальности.

2.23. Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.24. Шифр – совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

2.25. Шифрование – способ преобразования открытой информации в закрытую и обратно, для хранения в ненадежных источниках или передачи её по незащищенным каналам связи.

2.26. Шифровальные средства (средства криптографической защиты информации или СКЗИ) – Программно-техническое средство «КриптоПро CSP», осуществляющее криптографическое преобразование информации для обеспечения неизменности содержания и установления авторства электронных документов, а также конфиденциальности и контроля целостности информации.

2.27. Электронная подпись (далее – ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2.28. USB-Token – персональное средство аутентификации и защищенного хранения данных, аппаратно поддерживающее работу с сертификатами и электронной подписью (ЭП).

2.29. «Документы валютного контроля» – документы, связанные с проведением валютных операций, в том числе:

- «Ведомость банковского контроля» – документ, который формируется и ведется в электронном виде, в отношении контрактов, принятых на учет уполномоченным банком;

- **«Формы учета по валютным операциям»** – справка о подтверждающих документах Клиента, а также иные документы, предусмотренные действующим законодательством Российской Федерации и нормативными документами Банка России по валютному контролю.

2.30. «Документы зарплатного проекта» – экранные формы в модуле «Зарплатный проект» Системы, посредством которых осуществляется файловый обмен между Банком и организацией для проведения операций в рамках Договора зарплатного проекта, в том числе:

- **«Справочник «Сотрудники организации»»** – экранная форма в модуле «Зарплатный проект» Системы, которая содержит список работников организации, которым выпущены карты в рамках Договора зарплатного проекта, на основании которого формируются Документы на выпуск новых карт/ увольнение сотрудников/ расширение справочника «Сотрудники организации», Зарплатная ведомость; Справочник обновляется на ежедневной основе в автоматическом режиме, а также по запросу организации в ручном режиме.
- **«Зарплатная ведомость»** – экранная форма в модуле «Зарплатный проект» Системы, посредством которой осуществляется передача в Банк **Файла на зачисление**, оформленного в соответствии с требованиями Договора зарплатного проекта, необходимого для обеспечения перечисления заработной платы и иных платежей на счета физических лиц – работников организации;
- **«Документ на выпуск карт»** – экранная форма в модуле «Зарплатный проект» Системы, посредством которой осуществляется передача в Банк Файла на выпуск карт, оформленного в соответствии с требованиями Договора зарплатного проекта, на основании которого осуществляется выпуск расчетных банковских карт и открытие текущих счетов для расчетов с использованием карт работникам организации;
- **«Документ на увольнение сотрудников»** – экранная форма в модуле «Зарплатный проект» Системы, посредством которой осуществляется передача в Банк Файла уволенных работников, оформленного в соответствии с требованиями Договора зарплатного проекта, на основании которого осуществляется уведомление Банка об увольнении работников организации, которым выпущены расчетные банковские карты в рамках Договора зарплатного проекта и перевод карт на соответствующие тарифы, указанные в Договоре зарплатного проекта;
- **«Документ на расширение справочника «Сотрудники организации»»** – экранная форма в модуле «Зарплатный проект» Системы, посредством которой осуществляется передача в Банк Файла на расширение справочника «Сотрудники организации», оформленного в соответствии с требованиями Инструкции по работе в модуле «Зарплатный проект» Системы «Клиент-Банк», который позволяет добавлять в справочник «Сотрудники организации» карты, выпущенные в рамках Договора зарплатного проекта других организаций, в случае если работник трудоустроен по совместительству.

2.31. «Ответственное лицо Банка по ВК» – сотрудник Банка, уполномоченный на основании распорядительного документа по Банку осуществлять от имени Банка действия по валютному контролю, предусмотренные действующим законодательством Российской Федерации.

2.32. Аналог собственноручной подписи ответственного лица Банка (АСП) – персональный идентификатор Банка, являющийся контрольным параметром правильности составления всех реквизитов документов и неизменности их содержания.

3. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ РАСЧЕТОВ ПО ЭЛЕКТРОННОЙ СИСТЕМЕ «КЛИЕНТ-БАНК» С ВСТРОЕННЫМИ СЕРТИФИЦИРОВАННЫМИ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

3.1.Клиент предоставляет в **Банк** Заявку на подключение к Электронной системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации» (Приложение № 7, № 7а (в зависимости от предоставленных прав подписи) к Правилам), Заявление на регистрацию в Удостоверяющем центре Банка (Приложение № 8 к Правилам), Заявка на установление ограничения на подключение к электронной системе «Клиент-Банк» по сетевым адресам (Приложение № 6 к Правилам), в случае если **Клиент** ограничения установил. После проверки данных документов, Клиент получает конверт с логином и паролем и ключевые носители и подписывает Расписку о получении обезличенного дистрибутива подключения к системе Клиент-Банк и ключевых носителей USB-Token (Приложение №3 к Правилам)

3.2.Клиент обеспечивает комплектование аппаратного обеспечения для программного комплекса Системы, а также предоставляет каналы связи и помещение согласно требованиям, изложенным в разделе № 4 Правил.

3.3.Формирование ключей шифрования и электронной подписи **Клиента** является непременным элементом процедуры его подключения к Системе и осуществляется после заключения Договора (присоединения к Правилам), в соответствии с порядком, указанным в настоящем разделе Правил, и регистрации уполномоченного лица **Клиента** в Удостоверяющем центре ПАО «МТС-Банк».

3.4.Полномочия лиц, осуществляющих формирование ключей ЭП (и шифрования), определяются на основании Заявки на подключение к Электронной системе «Клиент-Банк» (Приложения №7 ,№ 7а к Правилам).

3.5.При подключении к Системе формирование ключей **Клиента** и Сертификатов ключей проверки ЭП осуществляется **Клиентом** самостоятельно на своем рабочем месте с помощью обезличенного дистрибутива подключения к системе Клиент-Банк, используя Руководство пользователя.

3.6.При генерации ключей ЭП на своем рабочем месте **Клиент** отправляет в **Банк** запрос на выпуск Сертификата. Перед получением Сертификата ключа проверки ЭП **Клиент** обязан заверить бланки Сертификатов открытых ключей (Приложение №4 к Правилам), переданные ему из **Банка**, подписью уполномоченного лица (владельца Сертификата ключа подписи), скрепить оттиском печати и передать экземпляры в **Банк**.

3.7.Бланки Сертификатов открытых ключей **Клиента** и **Банка** распечатываются в 2(двух) экземплярах.

3.8. До начала использования Сертификатов ключей проверки ЭП для работы в Системе бланки Сертификатов заверяются уполномоченными лицами **Клиента** и **Банка**. По одному экземпляру заверенных бланков Сертификатов открытых ключей хранится и используется **Клиентом** и **Банком**.

3.9.Наличие на бланках Сертификатов открытых ключей собственноручных подписей уполномоченных лиц **Клиента** и **Банка**, а также оттисков печатей означает обязательство обозначенных организаций использовать для проверки ЭП электронных документов и их шифрования исключительно данные ключи в период их действия.

3.10.Клиент обязан производить периодическую (плановую) замену используемых ключей ЭП (и шифрования) в срок, указанный на бланке Сертификата открытого ключа.

3.11.При самостоятельной смене ключей ЭП на своем рабочем месте **Клиент** отправляет в **Банк** запрос на выпуск Сертификата. Перед получением нового Сертификата ключа проверки ЭП **Клиент** обязан заверить два бланка нового сертификата открытого ключа подписью уполномоченного лица (владельца Сертификата ключа подписи), скрепить оттиском печати и передать экземпляры в **Банк**.

3.12.Банк передает **Клиенту** всю необходимую документацию по СКЗИ «КриптоПро CSP» и оформляет «Акт приема-передачи» (Приложение № 2 к Правилам).

3.13.Обслуживание системы «Клиент-Банк» начинается после подписания **Клиентом** Акта

приема-передачи, бланков сертификатов открытых ключей на бумажном носителе и предоставления их в **Банк**.

3.14. Если в результате проверки обнаружена неработоспособность (несовместимость) технических или программных средств, или причиной неработоспособности является низкое качество линий связи, **Банк** представляет **Клиенту** рекомендации по комплектации рабочего места техническими и программными средствами, **Клиент** следует этим рекомендациям и принимает меры по улучшению качества линий связи. В случае, если **Клиент** отказывается следовать рекомендациям **Банка**, то **Банк** оставляет за собой право расторгнуть Договор в порядке, установленном в разделе 17 настоящих Правил.

3.15. **Клиент** в Системе «Клиент-Банк» подготавливает для **Банка** электронные документы установленной формы. При этом он заполняет соответствующие реквизиты в сформированной электронной форме документа. За правильное заполнение платежных и иных реквизитов документа несет ответственность **Клиент**.

3.16. После подготовки электронного документа **Клиентом** производится его подписание ЭП, шифрование и отправка в **Банк** по каналам связи. Порядок подготовки, контроля и отправки электронных документов в **Банк** подробно описан в документации на программное обеспечение Системы.

3.17. **Клиент** может отозвать свой электронный документ до его исполнения **Банком** (до наступления безотзывности перевода денежных средств), создав в Системе электронный документ «Запрос на отзыв документа» и выбрав из списка электронный документ для отзыва. Электронный документ «Запрос на отзыв документа» шифруется и подписывается ЭП **Клиента**. Так же **Клиент** может направить заявление на отзыв в текстовом сообщении Системы, с указанием реквизитов, необходимых для осуществления отзыва (номер, дата составления, сумма расчетного документа, наименование получателя средств). Текстовое сообщение на отзыв шифруется и подписывается ЭП **Клиента**.

Банк не позднее рабочего дня, следующего за днем поступления заявления об отзыве, направляет **Клиенту** уведомление в электронном виде об отзыве с указанием даты, возможности (невозможности в связи с наступлением безотзывности перевода денежных средств) отзыва распоряжения (электронного документа). Заявление об отзыве служит основанием для аннулирования **Банком** распоряжения (электронного документа).

3.18. В рамках настоящих Правил осуществляются следующие процедуры приема ЭД к исполнению:

- процедура удостоверения права распоряжения денежными средствами (удостоверение права использования электронного средства платежа) осуществляется автоматически посредством Системы «Клиент-Банк» при сеансе связи при передаче ЭД **Клиентом** в **Банк** путем проверки ЭП на удостоверение права распоряжения денежными средствами;
- процедура контроля целостности распоряжений осуществляется Системой «Клиент-Банк» автоматически перед отправкой **Клиентом** в **Банк** ЭД на этапе заполнения ЭД **Клиентом**, положительный результат контроля целостности подтверждается возможностью проставления ЭП на ЭД;
- процедура структурного контроля распоряжений осуществляется Системой «Клиент-Банк» автоматически путем проверки соответствия ЭД форме, установленной Системой «Клиент-Банк» и наличия заполнения полей формы ЭД необходимым количеством символов и реквизитов;
- процедура контроля значений реквизитов распоряжений осуществляется Системой «Клиент-Банк» и Автоматизированной банковской системой автоматически путем проверки в ЭД реквизитов, их допустимости и соответствие требованиям законодательства;
- процедура контроля наличия согласия третьего лица на распоряжение денежными средствами **Клиента** осуществляется в случаях, установленных законодательством и договором, автоматически посредством Системы «Клиент-Банк» путем проверки наличия ЭП третьего лица (акцепта третьего лица) на ЭД; соответствующая ЭП предоставляется третьему лицу на основании оформленной Заявки по форме Приложения № 7а к настоящим Правилам;
- процедура контроля достаточности денежных средств осуществляется многократно Автоматизированной банковской системой путем автоматической проверки достаточности денежных средств на банковском счете **Клиента**, исходя из остатка денежных средств, находящихся на банковском

счете Клиента на момент приема ЭД с учетом сумм денежных средств, списанных с банковского счета Клиента и зачисленных на его банковский счет до определения достаточности денежных средств на банковском счете Клиента, а также с учетом сумм наличных денежных средств, выданных с банковского счета Клиента и зачисленных на его банковский счет до определения достаточности денежных средств на банковском счете Клиента;

- процедура контроля за своевременностью представления Клиентом документов, необходимых для фиксации информации в соответствии с требованиями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и сомнительными операциями, осуществляемыми **Клиентом** по банковскому счету осуществляется в порядке, установленном Федеральным законом от 07.08.2001 № 115-ФЗ, нормативными актами Банка России и разработанными в соответствии с ними внутренними нормативными документами Банка;
- контроль за подозрительными операциями осуществляется в порядке, установленном Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», нормативными актами Банка России и разработанными в соответствии с ними внутренними нормативными документами Банка;

3.19. При положительном результате прохождения **всех** процедур приема ЭД к исполнению Банк направляет в день принятия ЭД к исполнению Клиенту уведомление в электронном виде посредством Системы о приеме данного ЭД к исполнению с указанием даты принятия ЭД к исполнению.

3.20. ЭД, прошедшие все процедуры приема к исполнению, подлежат исполнению не позднее дня, следующего за днем поступления в Банк соответствующего ЭД, если иной срок не предусмотрен законом, изданными в соответствии с ним банковскими правилами или Договором, заключенным между Клиентом и Банком.

В тот же срок Банк направляет Клиенту посредством Системы ЭД, содержащие распоряжения Клиента и иные расчетные документы о списании денежных средств со счета Клиента, содержащие штамп «ПРОВЕДЕНО» (с указанием даты исполнения соответствующего распоряжения/ расчетного документа) и являющиеся подтверждением исполнения Банком распоряжений Клиента.

Ежедневно не позднее дня, следующего за днем совершения операций, Банк предоставляет посредством Системы выписку о проведении операций по счету/счетам Клиента (на основании распоряжений, переданных/поступивших в Банк посредством Системы или на бумажном носителе) и приложений к ней. При этом выписки на бумажном носителе в порядке, предусмотренном соответствующим Договором банковского счета, заключенным между Банком и Клиентом, по мере совершения операций не предоставляется.

Выписка на бумажном носителе (о совершении операций по счету за любой указанный Клиентом период времени) предоставляется Банком по требованию Клиента в качестве дубликата лицам, указанным в Карточке с образцами подписей и оттиска печати, а так же лицам, имеющим доверенность на получение выписок по счету/ счетам Клиента. Плата за предоставление дубликата выписки взимается Банком в соответствии с «Каталогом услуг и тарифов ПАО «МТС-Банк» для клиентов – юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, и Договором банковского счета.

Выписка на бумажном носителе за последний рабочий день года (по состоянию на 1 января года, следующего за отчетным), а также в иных случаях, предусмотренных законодательством Российской Федерации, предоставляется Банком Клиенту без взимания платы.

В случае помещения ЭД в очередь не исполненных в срок распоряжений, Банк направляет Клиенту уведомление в электронном виде с указанием в нем номера и суммы ЭД, а также даты помещения ЭД в очередь не исполненных в срок распоряжений.

3.21. При отрицательном результате процедур приема к исполнению ЭД **Банк** не принимает ЭД к исполнению и направляет **Клиенту** уведомление в электронном виде об аннулировании данного ЭД с указанием информации, позволяющей идентифицировать аннулируемое

распоряжение (даты, номера и суммы документа), даты его аннулирования, а также причины аннулирования в виде текстового комментария.

3.22. В рамках Системы прием платежных и служебно-информационных документов **Клиента** осуществляется **Банком** в автоматическом режиме круглосуточно, за исключением возможных технологических перерывов с 20-00 до 02-00 по московскому времени. Платежные документы по операциям в рублях и в иностранной валюте, принятые Банком, исполняются согласно установленного внутренним Приказом по **Банку** режима операционного обслуживания клиентов юридических лиц, но не позднее дня, следующего за днем поступления в **Банк** платежных документов, если иное не предусмотрено Договором, заключенным между **Банком** и **Клиентом**.

3.23. Информация об остатке денежных средств на счете предоставляется **Клиенту**:

- за предыдущий рабочий день – до 9-30 по московскому времени;
- текущая (актуальная) информация об остатке денежных средств по счету **Клиента** – в течение 15-20 минут после зачисления/списания денежных средств по счету.
- дополнительная информация об остатке денежных средств по счету предоставляется **Клиенту** по его запросу, **направленному** по Системе «Клиент-Банк».

3.24. В процессе сеансов связи **Клиент** получает информацию об этапах приема, контроля и прохождения ЭД в **Банке** путем смены статуса ЭД в Системе.

4. ТРЕБОВАНИЯ К КЛИЕНТАМ, ОСУЩЕСТВЛЯЮЩИМ ЭКСПЛУАТАЦИЮ СЕРТИФИЦИРОВАННЫХ ФСБ РОССИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Техническое обслуживание сертифицированных ФСБ России шифровальных средств могут осуществлять только организации, имеющие соответствующие лицензии ФСБ.

4.2. Уполномоченное лицо **Клиента** назначает ответственных должностных лиц из числа сотрудников **Клиента**, ответственных за сохранность ключей ЭП (и шифрования) и имеющих право работать с Системой.

4.3. Специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), должны обеспечивать Безопасность информации, СКЗИ и ключей ЭП (и шифрования), сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

4.4. Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры **Клиента**.

4.5. Для хранения защищенных носителей ключей ЭП (и шифрования), нормативной и эксплуатационной документации, помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого распорядительным документом **Клиента**.

4.6. Устанавливаемый руководителем **Клиента** порядок охраны помещений должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

4.7. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

4.8. Системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля за их вскрытием.

4.9. В целях противодействия получению несанкционированного доступа к секретным ключам ЭП (и шифрования), ключи ЭП (и шифрования) должны находиться только на защищенных

носителях (смарт-картах, USB-токенах и т.п.) у ответственных лиц. Размещение ключей в реестре операционной системы не допустимо.

4.10. Все защищенные носители с ключами ЭП (и шифрования) должны учитываться в специально выделенных для этих целей журналах.

4.11. Учет и хранение носителей закрытых ключей ЭП (и шифрования) осуществляется уполномоченными лицами Клиента, имеющими право подписи электронных платежей. Их не рекомендуется передавать на хранение и использование лицам, не имеющим право подписи электронных платежей.

4.12. Хранение носителей ключей ЭП (и шифрования) допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

4.13. При пересылке ключей ЭП (и шифрования), должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.

4.14. В случае отсутствия у ответственных за использование СКЗИ Клиента лиц индивидуального хранилища, ключи ЭП (и шифрования) по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

4.15. Клиент обязан не допускать появления в компьютере, на котором установлена Система «Клиент-Банк», компьютерных вирусов, программ-шпионов и других вредоносных программ для исключения несанкционированного перехвата ключевой информации и передачи ее третьим лицам. Для чего не рекомендуется с компьютера, на котором установлена Система «Клиент-Банк», посещать ресурсы интернет и пользоваться электронной почтой.

4.16. Клиент обязан производить регенерацию и замену ключей ЭП (и шифрования) не реже 1 раза в год, и каждый раз при изменении состава должностных лиц, уполномоченных распоряжаться счетом.

4.17. К работе с СКЗИ допускаются решением (распорядительным документом) руководителя Клиента только сотрудники, знающие правила их эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

4.18. Руководитель Клиента и лица, уполномоченные на осуществление эксплуатации шифровальных средств, должны иметь представление о возможных угрозах утечки секретной информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

4.19. В случае если при заключении Договора об обслуживании с использованием Системы «Клиент-Банк» у Клиента отсутствуют открытые в Банке действующие банковские счета, в рамках Договора об обслуживании с использованием Системы «Клиент-Банк» Клиенту будет доступен только модуль «Зарплатный проект». Если после заключения Договора Клиент заключит с Банком договор (договоры) банковского счета, ему предоставляется доступ к другим сервисам (видам обслуживания) в Системе в соответствии с настоящими Правилами при условии оформления документов, предусмотренных п.1.3. Правил (кроме Заявления о присоединении к Правилам обмена электронными документами по Системе «Клиент-Банк»).

5. ОБЯЗАТЕЛЬСТВА БАНКА

Банк обязуется:

5.1. Обеспечить четкое функционирование Системы в режиме 24x7 с возможностью проведения регламентных работ (технологических перерывов) в нерабочие дни или в будни в период с 20:00 до 02:00 по московскому времени не более 3 раз в месяц. В иное время при

возникновении сбоев в срок не более 1,5 часов обеспечить работоспособность Системы. При этом прием документов осуществляется в режиме, указанном в п.3.22. настоящих Правил.

5.2. Обеспечить **Клиента** после подписания настоящего Договора комплексом программных средств, обеспечивающих функционирование Системы, необходимой нормативно-технической документацией, а также документацией на используемую систему защиты информации.

5.3. Консультировать представителей **Клиента** работе в Системе в установленное внутренним Приказом по **Банку** время операционного обслуживания клиентов юридических лиц.

5.4. Принимать полученные по Системе электронные документы (пакеты электронных документов), оформленные в соответствии с Правилами.

5.5. Обеспечивать защиту информации в Системе от несанкционированного доступа с использованием средств криптографической защиты информации, сертифицированных ФСБ России. Для этого:

5.5.1. Сохранять конфиденциальность и подлинность используемых ключей ЭП (и шифрования) и паролей.

5.5.2. Протоколировать все случаи и попытки нарушения безопасности Системы. При возникновении таких случаев принимать все возможные меры для предотвращения и ликвидации их последствий вплоть до приостановления функционирования Системы.

5.5.3. В случае получения информации о компрометации ключей ЭП (и шифрования) **Клиента** заблокировать работу **Клиента** в Системе «Клиент-Банк» до завершения внеплановой смены ключей ЭП (и шифрования).

5.5.4. Обеспечивать сохранность и конфиденциальность информации, доверенной ему **Клиентом** в ходе практической деятельности в рамках настоящего Договора, в соответствии с действующим законодательством.

5.5.5. Своевременно информировать **Клиента** об изменениях порядка осуществления приема/передачи ЭД и другой информации по Системе. Оказывать консультационные услуги **Клиенту** по вопросам функционирования Системы и использования СКЗИ.

5.5.6. Соблюдать положения документов, регламентирующих функционирование Системы.

5.6. Предоставлять **Клиенту** выписки о проведении операций по счетам Клиента по Системе «Клиент-Банк» » в соответствии с п.3.20. настоящих Правил.

5.7. Предоставлять **Клиенту** новые версии программного обеспечения Системы в случае их замены без дополнительной оплаты, а также консультировать Клиента по телефону в случаях сбоев установленной у Клиента Системы в целях устранения последствий сбоев и восстановления нормального функционирования Системы.

5.8. Зарегистрировать уполномоченных лиц **Клиента** в Реестре Удостоверяющего Центра в соответствии с данными Заявления на регистрацию в Удостоверяющем центре (Приложение № 8 к Правилам), изготовить и передать **Клиенту** в электронном виде сертификаты ключей проверки ЭП (сертификаты ключей подписи).

5.9. Предоставить зарегистрированным уполномоченным лицам **Клиента** права доступа к Системе в соответствии с данными Заявок не позднее следующего рабочего дня после получения от **Клиента** заверенных владельцем сертификатов ключей подписи бланков сертификатов открытых ключей на бумажном носителе и «Акта приема-передачи» (Приложение №2 к Правилам), а так же подписать со стороны Банка и передать их **Клиенту**.

5.10. Незамедлительно информировать банк-корреспондент о списании денежных средств **Клиента** (по его информации) в результате несанкционированного доступа к банковскому счету указанного **Клиента** с предложением (просьбой) оказать содействие по возврату денежных средств (как ошибочно перечисленных, необоснованно списанных при несанкционированном доступе к счету).

5.11. Провести служебное расследование факта несанкционированного доступа к счету **Клиента** в установленном порядке с привлечением **Клиента**, проинформировать **Клиента** о результатах расследования.

6. ОБЯЗАТЕЛЬСТВА КЛИЕНТА

Клиент обязуется:

6.1. Представить **Банку** материалы и информацию, необходимые для подключения к Системе.

6.2. Оборудовать за свой счет автоматизированное рабочее место – АРМ «Клиент-Банк», в составе персонального компьютера с доступом к сети Интернет с операционной системой Microsoft Windows 7 и выше¹, а так же следующими характеристиками:

- объемом доступной памяти на жестком диске не менее 3 ГБ,
- наличием свободного USB-порта;
- программное обеспечение MS Internet Explorer версии 9.0 или выше;
- установленное и работающее лицензионное антивирусное ПО.

6.3. Назначить лиц, имеющих право работать с Системой и ответственных за сохранность ключей ЭП (и шифрования), подать Заявления на регистрацию в Удостоверяющем центре (Приложение № 8 к Правилам), произвести генерацию ключей в соответствии с руководством пользователя Системы (предоставленным **Банком Клиенту**), и подать запрос на выпуск сертификатов ключей проверки ЭП (и шифрования) должностных лиц, ответственных за работу с электронными документами в Системе.

6.4. Предоставить в **Банк** бланки сертификатов открытых ключей (Приложение №4 к Правилам), заверенные подписями зарегистрированных в Удостоверяющем центре лиц (владельцев сертификатов) и печатью **Клиента**. Бланки сертификатов открытых ключей формируются Банком, передаются **Клиенту** и заверяются Сторонами в двух экземплярах, по одному для каждой Стороны.

6.5. Строго соблюдать предусмотренные настоящими Правилами требования к подготовке и передаче ЭД.

6.6. Обеспечивать защиту Системы от несанкционированного доступа с использованием средств криптографической защиты информации, сертифицированных ФСБ России. Для этого выполнять требования, перечисленные в разделе 4 настоящих Правил, а также в Правилах на использование СКЗИ "КриптоПро CSP", передаваемых **Клиенту Банком**.

6.7. Незамедлительно извещать **Банк** обо всех случаях компрометации ключей ЭП (и шифрования) и выхода из строя носителей ключей ЭП **Клиента для их смены**, предоставив письмо об отзыве сертификата ключа подписи (Приложение № 5 к Правилам).

6.8. Немедленно сообщать службе техподдержки **Банка** о случаях несанкционированного доступа к счету и списания денежных средств по телефону номер 8(495)225-15-14.

6.9. По первому требованию **Банка** представлять информацию, подтверждающую подлинность (аутентичность) платежного документа, направленного с использованием Системы «Клиент-Банк» (в том числе, предоставлять платежный документ, направленный с использованием Системы «Клиент-Банк», на бумажном носителе с подписями лиц, уполномоченных распоряжаться счетом, и оттиском печати **Клиента** (при наличии)).

6.10. Соблюдать конфиденциальность информации, касающейся Системы.

6.11. Использовать предоставленные Банком средства электронной Системы только для целей, определенных настоящими Правилами.

6.12. **Клиент** обязуется использовать предоставленные шифровальные (криптографические) средства (СКЗИ) только в Системе и только на территории Российской Федерации, без права их продажи или передачи каким-либо другим способом третьим лицам. Все исключительные

¹ при условии совместимости соответствующей версии ОС с сертифицированной версией СКЗИ

права на Программное обеспечение СКЗИ, его модификации и переводы сохраняются за Правообладателем (ООО «Крипто-Про»). **Банк**, имея соответствующие полномочия от Правообладателя, предоставляет **Клиенту** неисключительные (ограниченное) право (Лицензию) на использование Программного обеспечения СКЗИ. Стоимость лицензии на ПО СКЗИ КриптоПро CSP 4.0 включена в стоимость подключения системы «Клиент-Банк» со встроенными средствами криптографической защиты информации КриптоПро CSP². Клиент не приобретает каких-либо прав на Программное обеспечение, за исключением указанных в Правилах.

6.13. В случае уведомления **Банком Клиента** о смене программного обеспечения и/или смене сертификатов ключей обеспечить меры для их своевременного получения и установки в соответствии с Правилами.

6.14. Оплатить услуги Банка за подключение к системе «Клиент-Банк» каждого рабочего места в соответствии с «Каталогом услуг и тарифов ПАО «МТС-Банк» для клиентов – юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой» (далее – Тарифы).

6.15. Оплатить услуги **Банка** по изготовлению сертификатов ключей проверки ЭП и регистрации их в Системе «Клиент-Банк» в соответствии с Тарифами.

6.16. Своевременно вносить абонентскую плату за сопровождение и обслуживание Системы «Клиент-Банк» на каждом рабочем месте в соответствии с Тарифами.

6.17. Не позднее одного рабочего дня с момента передачи бланков сертификатов открытых ключей (Приложение № 4 к Правилам) подписать со своей стороны «Акт приема-передачи» (Приложение №2 к Правилам) и передать в Банк.

6.18. Производить смену ключей шифрования и ЭП лиц, ответственных за работу с электронными документами в Системе, не менее 1 (Одного) раза в год, и предоставлять в Банк бланки новых сертификатов) (Приложения №4 к Правилам) в 2(двух) экземплярах.

6.19. В случае изменения данных владельца сертификата (ФИО, наименования организации, юридического адреса), Клиент должен предоставить в **Банк** новую Заявку на подключение к Системе, оформленную согласно Приложению № 7 к Правилам, или Приложению № 7а (в случае, когда в соответствии с федеральным законом и договором для распоряжения денежными средствами Клиента необходимо согласие третьего лица):

- подать Заявления на их регистрацию в Удостоверяющем центре (Приложение № 8 к Правилам);
- предоставить заявление об отзыве сертификатов ключей проверки ЭП лиц, у которых меняются данные, с указанием причины отзыва (изменение регистрационных данных);
- произвести для них генерацию ключей, подать запрос на выпуск Сертификатов ключей проверки ЭП (и шифрования), предоставить новые бланки сертификатов открытых ключей, заверенные подписью и печатью.

6.20. В случае изменения полномочий или состава лиц, уполномоченных подписывать электронные документы, **Клиент** одновременно с новой карточкой с образцами подписей и оттиска печати/ в случае изменения состава уполномоченных лиц, не включенных в карточку с образцами подписей и оттиска печати (в случаях, предусмотренных в разделах 12, 13 настоящих Правил) должен предоставить в **Банк** новую Заявку на подключение к Системе, оформленную согласно Приложению № 7 к Правилам, или Приложению № 7а (в случае, когда в соответствии с федеральным законом и договором для распоряжения денежными средствами Клиента необходимо согласие третьего лица):

- подать Заявления на их регистрацию в Удостоверяющем центре (Приложение № 8 к Правилам);

² стоимость лицензии на иную сертифицированную версию данного ПО согласно установленным тарифам Банка

- предоставить заявление об отзыве сертификатов ключей проверки ЭП лиц, исключенных из карточки с образцами подписей и оттиска печати/ прекращения действия распорядительного документа/ отмены доверенности, на основании которых лица были уполномочены подписывать ЭД без включения в карточку с образцами подписей и оттиска печати (в случаях, предусмотренных в разделах 12, 13 настоящих Правил) (Приложение №5 к Правилам);
- получить по Расписке (Приложение №3 к Правилам) новые защищенные ключевые носители USB-Token для вновь назначенных уполномоченных лиц.
- произвести для них генерацию ключей, подать запрос на выпуск Сертификатов ключей проверки ЭП (и шифрования), предоставить новые бланки сертификатов открытых ключей заверенные подписью и печатью.

6.21. Клиент обязан предоставлять информацию, необходимую для исполнения Банком требований Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», включая информацию о своих выгодоприобретателях и бенефициарных владельцах.

7. ПРАВА БАНКА

Банк имеет право:

7.1. Вносить изменения в «Каталог услуг и тарифов ПАО «МТС-Банк» для клиентов – юридических лиц, индивидуальных предпринимателей, физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой» (далее – Тарифы) в части размера комиссий, уплачиваемых Клиентом Банку за обслуживание в Системе «Клиент-Банк», срока и порядка оплаты указанных комиссий, с предварительным уведомлением Клиента по Системе «Клиент-Банк», размещения информации в местах обслуживания **Клиентов Банка**, размещения на корпоративном Интернет-сайте Банка www.mtsbank.ru не менее, чем за 5(пять) рабочих дней до даты вступления в силу соответствующих изменений.

7.2. Отказать **Клиенту** в совершении операций по счету с использованием ЭД в случае отрицательного результата процедур приема к исполнению ЭД, предусмотренных Порядком взаимодействия участников расчетов по системе «Клиент-Банк» с встроенными сертифицированными средствами криптографической защиты информации (п. 3.19.Раздел 3 настоящих Правил).

7.3. В случае возникновения у **Банка** технических неисправностей или других обстоятельств, препятствующих использованию Системы, в одностороннем порядке приостановить работу с **Клиентом** через Систему «Клиент-Банк» до момента устранения неисправностей. Все платежные документы в этом случае должны передаваться в **Банк** и **Клиенту** на бумажных носителях в установленном порядке. Действие данного пункта не должно противоречить п. 5.1. настоящих Правил.

7.4. При наличии у Банка сомнений в подлинности (аутентичности) платежного документа, поступившего с использованием Системы, направить письменный запрос Клиенту (с курьером/ посредством факсимильной связи/ по Системе «Клиент-Банк») или провести переговоры с Клиентом по телефону о подтверждении подлинности документа. В случае подтверждения Клиентом подлинности платежного документа, Банк выполняет операцию по нему не позднее банковского дня, следующего за днем получения Банком платежного документа.

7.5. Отключить **Клиента** от Системы «Клиент-Банк» в случаях выявления фактов допуска **Клиентом** к Системе «Клиент-Банк» третьих лиц; временно блокировать доступ Клиента к Системе «Клиент-Банк» в случае поступления информации о зачислении на банковский счет **Клиента** денежных средств, списанных в результате несанкционированного доступа к счетам третьих лиц (в Банке или в других кредитных организациях).

7.6. Расторгнуть Договор об обслуживании с использованием Системы «Клиент-Банк», заключенный в соответствии с настоящими Правилами, в одностороннем порядке в случае неисполнения **Клиентом** обязательств по оплате услуг **Банка** по сопровождению и обслуживанию Системы «Клиент-Банк» в соответствии с Тарифами путем направления **Клиенту** письменного уведомления в порядке, предусмотренном п.17.2. настоящих Правил. Решение о способе отправки уведомления (почтовым отправлением или по Системе «Клиент-Банк») принимается **Банком**.

7.7. При выявлении сомнительных операций, осуществляемых **Клиентом** по счету, а также в случае отказа **Клиента** от предоставления **Банку** запрашиваемых документов (в случае не предоставления таких документов), после предварительного предупреждения **Клиента** отказать ему в приеме распоряжений на проведение операций по банковскому счету, направленных в **Банк** с использованием Системы «Клиент-Банк». В этом случае **Клиент** вправе направлять в Банк надлежащим образом оформленные расчетные документы на бумажном носителе.

7.8. Требовать от **Клиента** в рамках осуществления деятельности по реализации положений Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» предоставления в срок, указанный **Банком**, документов, связанных с проведением **Клиентом** банковских операций и подтверждающих их действительность и экономическую обоснованность (в т.ч. заверенные надлежащим образом копии договоров, на основании которых производится зачисление/списание денежных средств, счетов-фактур, спецификаций и др.), а также копий документов, заверенных надлежащим образом, содержащих сведения о выгодоприобретателях и бенефициарных владельцах **Клиента**.

7.9. Отказать в выполнении распоряжения **Клиента** о совершении операции, по которой не представлены документы, необходимые для фиксирования информации в соответствии с требованиями Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а также в случае, если у работников **Банка** возникают подозрения, что операция совершается в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

7.10. Расторгнуть Договор об обслуживании с использованием Системы «Клиент-Банк», заключенный в соответствии с настоящими Правилами, в случае принятия в течение календарного года двух и более решений об отказе в выполнении распоряжения **Клиента** о совершении операции по основаниям, указанным в п.7.9. настоящих Правил.

8. ПРАВА КЛИЕНТА

Клиент имеет право:

8.1. Вносить предложение о смене сертификатов ключей в соответствии с настоящими Правилами.

8.2. В случае возникновения у **Клиента** технических неисправностей или других обстоятельств, препятствующих использованию ЭД, обратиться в **Банк** с письмом, содержащим мотивированную просьбу о приостановлении его работы в Системе на определенный срок. Все документы в этом случае должны передаваться в **Банк** и **Клиенту** на бумажных носителях в установленном порядке. Изменение порядка передачи документов вступает в силу с момента получения Банком уведомления **Клиента**.

8.3. Взаимодействовать с **Банком** в ходе расследования факта несанкционированного доступа к счету **Клиента**, получать от Банка информацию о результатах расследования.

9. ОБЯЗАННОСТИ СТОРОН

9.1 Стороны обязуются обеспечить соблюдение порядка хранения защищенных носителей с ключевой информацией СКЗИ и условия хранения и использования программного обеспечения СКЗИ, исключающие порчу и утрату защищенного носителя, а также их использование любыми другими лицами.

9.2 Сторона, допустившая утрату контроля за носителем с ключевой информацией СКЗИ, независимо от наличия или отсутствия сведений о его несанкционированном использовании, незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля защищенный носитель с ключевой информацией СКЗИ не подлежит дальнейшему использованию.

10. ПЕРЕДАЧА ПРАВ

10.1. Ни одна из Сторон не может передавать свои права и обязательства по Договору, заключенному в соответствии с настоящими Правилами третьим лицам.

11. ПОРЯДОК РАСЧЕТОВ

11.1. Клиент оплачивает услуги **Банка** за обслуживание в Системе «Клиент-Банк» в размере и сроки, указанные в Тарифах, и в соответствии с настоящими Правилами. В случае неисполнения **Клиентом** обязательств по оплате **Банку** услуг и внесению абонентской платы **Банк** имеет право без дополнительного распоряжения Клиента списать с расчетного счета, а при невозможности списания с расчетного счета - с любого банковского счета Клиента, открытого в **Банке**, сумму денежных средств в размере стоимости услуг/абонентской платы.

11.2. Абонентская плата за первый месяц обслуживания в Системе оплачивается одновременно с оплатой стоимости услуг по подключению Системы «Клиент-Банк».

11.3. Абонентская плата за полный и неполный месяц обслуживания (за первый месяц обслуживания при подключении Системы «Клиент-Банк» и за последний месяц обслуживания при расторжении Договора) оплачивается в размере, установленном Тарифами за полный месяц. Абонентская плата за месяц расторжения Договора оплачивается в день расторжения Договора путем списания **Банком** без дополнительного распоряжения **Клиента** суммы абонентской платы с расчетного счета **Клиента**.

12. ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПО ДОКУМЕНТАМ ВАЛЮТНОГО КОНТРОЛЯ

12.1. Клиент подписывает документы для валютного контроля, направляемые в **Банк** посредством Системы «Клиент-Банк», ЭП **Клиента**.

12.2. Документы для валютного контроля, требование о представлении которых предусмотрено нормативными документами Банка России, Клиент передает в **Банк** посредством Системы «Клиент-Банк» как сформированные в электронном виде, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

12.3. Датой предоставления **Клиентом** в **Банк** документов и информации по валютному контролю является :

- для Форм учета по валютным операциям – дата, указанная в штампе «Получено по системе электронных платежей. Подписи проверены», проставляемом автоматически Системой «Клиент-Банк» на стороне **Банка** при получении **Банком** документов;
- для Ведомостей банковского контроля и иных документов, предусмотренных действующим валютным законодательством Российской Федерации – дата, указанная в штампе «Получено по системе электронных платежей. Подписи проверены»,

автоматически проставляемом Системой «Клиент-Банк» на сопроводительном/произвольном документе, созданном **Клиентом** в Системе «Клиент-Банк» и содержащем информацию и/или прикрепленный файл (файлы).

12.4. Датой предоставления Клиентом в Банк документов валютного контроля считается день поступления документов в Банк посредством Системы Клиент-Банк» в период времени операционного обслуживания Клиентов.

12.5. При поступлении документов валютного контроля в **Банк** после указанного в п.12.4. настоящих правил времени, датой предоставления **Клиентом** в **Банк** документов будет считаться следующий день, операционного обслуживания Клиентов

12.6. Документы валютного контроля, полученные **Банком** от **Клиента**, должны быть четкими, понятными и полными.

12.7. Документы валютного контроля, направляемые **Клиенту** посредством Системы «Клиент-Банк», подписываются со стороны **Банка** аналогом собственноручной подписи Ответственного лица Банка по ВК (АСП) в соответствии с внутренними процедурами **Банка**.

12.8. Датой принятия **Банком** Форм учета по валютным операциям считается дата проставления окончательного статуса Ответственным лицом Банка по ВК на принятом документе в Системе «Клиент-Банк».

12.9. Датой принятия **Банком** контракта на учет считается дата направления Клиенту соответствующей информации Ответственным лицом Банка по ВК посредством Системы «Клиент-Банк».

12.10. **Банк** имеет право отказаться от принятия Документов валютного контроля **Клиента** в случаях, установленных действующим законодательством Российской Федерации, а так же в случае если Документы валютного контроля не соответствуют требованиям, указанным в пункте 12.6 настоящих Правил.

12.11. Датой возврата **Банком** **Клиенту** не принятых Документов валютного контроля является :

- для Форм учета по валютным операциям – дата проставления финального статуса об отказе в принятии Банком документа;
- для внешнеторговых контрактов (договоров займа, кредитных договоров), для Ведомостей банковского контроля и иных документов – автоматически сформированная дата сопроводительного/ произвольного документа, созданного и направленного **Клиенту** Ответственным лицом Банка по ВК по электронной системе «Клиент-Банк» , содержащего информацию и/или прикрепленный файл (файлы) с указанием причины возврата.

12.12. При направлении **Клиенту** Документов валютного контроля посредством Системы «Клиент-Банк» могут передаваться как документы, сформированные посредством Системы, так и полученные с использованием сканирующих устройств изображения документов, оформленных первоначально на бумажном носителе.

12.13. В случае если Документы валютного контроля содержат приложения в форме вложений, Стороны настоящим признают, что наличие надлежащего аналога собственноручной подписи на Документе валютного контроля означает подписание тем же аналогом собственноручной подписи соответствующей Стороны всех имеющихся приложений в форме вложения к такому Документу валютного контроля.

12.14. В случае если произвольный/сопроводительный документ, созданный в Системе, содержит приложения в форме вложений, Стороны настоящим признают, что наличие надлежащего аналога собственноручной подписи на указанном произвольном/сопроводительном документе означает подписание тем же аналогом собственноручной подписи соответствующей Стороны всех имеющихся приложений в форме вложения к такому произвольному/ сопроводительному документу.

12.15. Получение **Клиентом** от Банка Документов валютного контроля посредством

электронной системы «Клиент-Банк» исключает повторное предоставление **Банком** Клиенту Документов валютного контроля на бумажном носителе.

13. ПОРЯДОК ХРАНЕНИЯ И УНИЧТОЖЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И СЕРТИФИКАТОВ КЛЮЧЕЙ

13.1. Банк и Клиент осуществляют хранение электронных документов, подписанных ЭП, соответствующих сертификатов ключей в электронной форме в течение 5 лет.

13.2. Банк и Клиент самостоятельно обеспечивают хранение архивов всех ЭД, подписанных ЭП, а также соответствующих сертификатов ключей.

13.3. Банк и Клиент обязаны обеспечить защиту архивов ЭД и сертификатов ключей от несанкционированного доступа в соответствии с требованиями, перечисленным в Разделе 4 настоящих Правил.

13.4. По истечении срока хранения ЭД и сертификатов ключей **Банк и Клиент** самостоятельно производят их уничтожение.

14. ОТВЕТСТВЕННОСТЬ СТОРОН

14.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему договору **Стороны** несут ответственность в соответствии с действующим законодательством Российской Федерации.

14.2. Банк не несет ответственности за неисполнение или ненадлежащее исполнение поручений **Клиента** в случаях, указанных в п. 7.3. настоящих Правил, из-за нарушения **Клиентом** положений настоящих Правил, а также в случаях, предусмотренных законодательством Российской Федерации.

14.3. Банк не несет ответственности за списание средств со счета **Клиента** в случае, если по причинам, не зависящим от **Банка**, электронные платежные документы были отправлены в **Банк** лицами, не несущими ответственность за сохранность ключей ЭП (и шифрования), не имеющими право работать с Системой, при условии, что электронные платежные документы были составлены правильно и соответствовали требованиям системы защиты от несанкционированного доступа и содержали правильные ЭП, а также, если **Банк** не был своевременно информирован об обстоятельствах, предусмотренных пунктами 6.6. и 8.3. настоящих Правил.

14.4. Банк не несет ответственности за невыполнение обязательств, предусмотренных настоящими Правилами в случае сбоя, возникших по причинам, независящим от Сторон.

14.5 Ответственность за правильность оформления первичных документов несет **Клиент**. **Банк** несет ответственность за сохранность электронных документов и своевременное исполнение платежных документов.

15. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И/ИЛИ ДОПОЛНЕНИЙ В ПРАВИЛА И/ИЛИ ТАРИФЫ

15.1. Банк вправе в одностороннем порядке вносить изменения и/или дополнения в настоящие Правила, в том числе утверждать новую редакцию Правил.

15.2. Банк информирует **Клиента** о внесении изменений/ дополнений в настоящие Правила, в том числе об утверждении новой редакции Правил **не менее, чем за 10 (десять)** календарных дней до даты вступления таких изменений/ дополнений/ новой редакции Правил в силу путем направления информационного сообщения по Системе «Клиент-Банк» и размещения на корпоративном Интернет-сайте Банка www.mtsbank.ru

15.3. Все изменения /дополнения вступают в силу, начиная со дня, следующего за днем истечения срока направления информационного сообщения по Системе «Клиент-Банк» и

размещения на корпоративном Интернет-сайте Банка www.mtsbank.ru, указанного в *пункте 15.2.* настоящих Правил.

15.4. Банк вправе в одностороннем порядке вносить изменения в Тарифы на обслуживание **Клиента** по системе «Клиент-Банк».

15.5. О внесении изменений в Тарифы Банк информирует **Клиента** не менее, чем за 5(пять) рабочих дней до даты вступления в силу изменений, вносимых в Тарифы, путем направления информационного сообщения по Системе «Клиент-Банк», размещения информации в местах обслуживания **Клиентов Банка**, размещения на корпоративном Интернет-сайте Банка www.mtsbank.ru.

15.6. В случае несогласия **Клиента** с изменениями/ дополнениями, внесенными Банком в Правила или Тарифы, новой редакцией Правил, **Клиент** имеет право расторгнуть Договор в порядке, предусмотренном пунктом 17.3. настоящих Правил.

16. ОПУБЛИКОВАНИЕ ИНФОРМАЦИИ

16.1. Под опубликованием информации в Правилах понимается размещение Банком информации на корпоративном Интернет-сайте Банка www.mtsbank.ru.

16.2. Моментом публикации Правил, планируемых изменений/дополнений Правил/ Тарифов считается момент их первого размещения на корпоративном Интернет-сайте Банка.

16.3. Банк не несет ответственности, если информация об изменении и/или дополнении Правил/ Тарифов, опубликованная в порядке и в сроки, установленные Правилами, не была получена и/или изучена и/или правильно истолкована **Клиентом**.

17. СРОК ДЕЙСТВИЯ ПРАВИЛ И ПОРЯДОК РАСТОРЖЕНИЯ

17.1. Договор считается заключенным и вступает в силу с даты проставления отметки о приеме уполномоченным сотрудником **Банка** на Заявлении о присоединении к Правилам обмена электронными документами по Системе «Клиент-Банк», составленном по форме Приложения №1 к настоящим Правилам, представленном **Клиентом** в **Банк** на бумажном носителе, и действует до момента его расторжения по соглашению сторон или в одностороннем порядке одной из Сторон в соответствии с пунктами 17.2.-17.4. настоящих Правил.

17.2. Договор об обслуживании с использованием Системы «Клиент-Банк», заключенный в соответствии с настоящими Правилами, может быть расторгнут в одностороннем порядке по инициативе **Банка**. Банк уведомляет об этом **Клиента** не позднее, чем за 15 (пятнадцать) календарных дней до даты расторжения путем направления письменного уведомления (заказным почтовым отправлением с уведомлением о вручении или по Системе «Клиент-Банк»). Договор считается расторгнутым с даты, указанной в уведомлении Банка.

17.3. Договор об обслуживании с использованием Системы «Клиент-Банк», заключенный в соответствии с настоящими Правилами, может быть расторгнут по инициативе **Клиента**. **Клиент** направляет в Банк письменное заявление о расторжении Договора, составленное по форме Приложения № 9 к настоящим Правилам. Договор считается расторгнутым с даты получения Банком Заявления.

17.4. Договор об обслуживании с использованием Системы «Клиент-Банк», заключенный в соответствии с настоящими Правилами, автоматически прекращает свое действие при расторжении договора(ов) банковского счета **Клиента**, заключенного(ых) между **Банком** и **Клиентом**.

18. ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПОСРЕДСТВОМ МОДУЛЯ «ЗАРПЛАТНЫЙ ПРОЕКТ»

18.1. Документы, направляемые Клиентом в Банк посредством модуля «Зарплатный проект» Системы «Клиент-Банк», подписываются ЭП Клиента, заключившего с Банком Договор зарплатного проекта.

18.2. Датой предоставления Клиентом в Банк Документов зарплатного проекта считается дата их направления в Банк после подписания ЭП в Системе лицом (и), наделенным (и) соответствующими полномочиями, в том числе на основании доверенности, оформленной Клиентом в порядке, установленном действующим законодательством Российской Федерации.

18.3. Предоставление Клиентом в Банк Документов зарплатного проекта, указанных в п.2.30. (за исключением Справочника «Сотрудники организации») и их исполнение/ отказ в приеме (исполнении) фиксируется Банком в виде статуса документа в Системе «Клиент-Банк»: «Новый»/ «Импортирован»/ «В обработке»/ «Исполнен»/ «Отказан АБС». Статус документа меняется в зависимости от действий Клиента по предоставлению документа в Банк и действий Банка по приему и исполнению документа. Полное описание статусов приведено в Инструкции по работе в модуле «Зарплатный проект» Системы.

18.4. Банк имеет право отказаться от принятия Документов зарплатного проекта Клиента в случаях, установленных Договором зарплатного проекта.

19. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ И ДОКАЗАТЕЛЬСТВА ПРИНАДЛЕЖНОСТИ ЭП ПРИ РАЗБОРЕ КОНФЛИКТНЫХ СИТУАЦИЙ

19.1. В случае возникновения споров по настоящему Договору или в связи с ним, Банк и Клиент примут все меры к их разрешению на взаимоприемлемой основе путем переговоров и действий в соответствии с законодательством Российской Федерации.

19.2. Разбор конфликтной ситуации выполняется по инициативе любого участника Системы и состоит из:

- предъявления претензии одной из сторон другой;
- формирования комиссии для рассмотрения конфликтной ситуации;
- разбора конфликтной ситуации.

19.3. Претензии друг к другу рассматриваются Сторонами на основании официально врученных уведомлений в письменном виде.

19.4. Стороны вправе решать возникающие претензии в рабочем порядке. По факту претензии Стороны проводят внутреннее расследование и официально информируют друг друга о его результатах в течение 14 (четырнадцати) календарных дней с даты получения претензии. Сторона, предъявившая претензию, в срок 5 (пять) рабочих дней после получения результатов расследования от другой Стороны, должна рассмотреть достаточность представленных объяснений и направить официальное уведомление о снятии претензии или предложение о создании комиссии по разрешению спорной ситуации.

19.5. В случае если хотя бы одна из Сторон при возникновении спора:

- высказывает недоверие к составу и формату электронных документов, хранящихся в локальном архиве рабочего места Клиента или Банка, или
- высказывает недоверие к программному обеспечению, функционирующему на данном рабочем месте, или
- не удовлетворена результатами рассмотрения претензии в рабочем порядке, то Стороны обязаны сформировать комиссию для рассмотрения конфликтной ситуации. Целью работы комиссии является установление правомерности и обоснованности претензии, а также установление, если необходимо, подлинности и авторства спорного документа.

19.6. В состав комиссии для рассмотрения конфликтной ситуации входит равное количество, но не менее двух, представителей от каждой из Сторон, определяемых Сторонами самостоятельно. При необходимости, по согласованию Сторон, к работе комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, а так же эксперт – представитель Разработчика СКЗИ «КриптоПро CSP». Оплата участия в работе комиссии представителя Разработчика производится Банком за счет Стороны, предъявляющей претензию. Право представлять соответствующую Сторону в комиссии должно подтверждаться доверенностью, выданной каждому представителю на согласованный Сторонами срок работы комиссии.

19.7. Комиссия определяет, включая, но, не ограничиваясь, следующее:

- предмет разногласий на основании письма Стороны-инициатора разбирательства и разъяснений Сторон;
- правомерность предъявления претензии на основании текста заключенного Договора (настоящих Правил и Приложений к ним);
- документы в электронной форме, относящиеся к предмету разногласий;
- идентичность открытых ключей Клиента или Банка;
- идентичность электронного документа документу на бумажном носителе, сформированному в Банке;
- истинность электронной подписи электронного документа;
- наличие и содержание подтверждения по электронному документу;
- даты и время поступления, отправки электронного документа и подтверждения по нему;
- исправность используемых ключевых носителей.

19.8. Стороны договариваются, что для разбора конфликтных ситуаций комиссия принимает на рассмотрение электронные документы и подтверждения по ним и обязана использовать следующие, признаваемые сторонами, эталонные данные:

- данные электронного архива принятых, отправленных документов;
- данные базы данных регистрационных записей (журнал регистрации приема и отправки электронных документов);
- подписанные сторонами оригиналы бланков Сертификатов открытых ключей Сторон;
- хранимое у Банка программное обеспечение системы «Клиент-Банк».

19.9. Результат работы комиссии оформляется Актом, в котором определяются последующие действия Сторон. Оспаривание результатов работы комиссии выполняется в установленном действующим законодательством Российской Федерации порядке.

19.10. Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов экспертной комиссии.

19.11. Экспертиза осуществляется в три этапа:

- Этап 1. Подготовка оборудования и программного обеспечения и тестирование их работоспособности;
- Этап 2. Контроль целостности оспариваемого электронного документа путем проверки ЭП при помощи Сертификата открытого ключа ЭП, представленного Банком;
- Этап 3. Аутентификация отправителя оспариваемого электронного документа путем проверки принадлежности, актуальности и целостности Сертификата, использованного комиссией для проверки ЭП.

19.12. Подготовка и проверка работоспособности оборудования и программного обеспечения проводятся в следующем порядке:

- производится конфигурирование операционной системы, осуществляется проверка предоставленного Банком персонального компьютера на предмет отсутствия вирусов и программных закладок;
- производится установка эталонного программного обеспечения СКЗИ «КриптоПро CSP». Для установки эталонного программного обеспечения СКЗИ «КриптоПро CSP» используется дистрибутив, представленный Разработчиком;
- членам экспертной комиссии предоставляется возможность убедиться в работоспособности, установленного программного обеспечения путем проведения тестов, в порядке, предусмотренном документацией на СКЗИ «КриптоПро CSP».

19.13. Контроль целостности оспариваемого электронного документа производится посредством стандартной процедуры проверки ЭП, предусмотренной СКЗИ «КриптоПро CSP». Проверка осуществляется на Сертификате ЭП, файл которого предъявляется Банком комиссии на защищенном носителе.

19.14. Для доказательства подлинности (принадлежности, актуальности и целостности) Сертификата, использованного для проверки ЭП, которой подписан оспариваемый документ, Банк должен предъявить членам комиссии заверенный уполномоченными лицами Клиента и Банка бумажный документ открытого ключа (сертификата).

Примечание.

Проверка принадлежности, актуальности и целостности Сертификата, подтвержденного письменным документом, проводится путем визуальной сверки членами экспертной комиссии распечатки файла Сертификата, записанного на представленном Банком съемном носителе и реквизитов Сертификата, зафиксированных в бумажном документе.

19.15. Подтверждением подлинности оспариваемого электронного поручения является единовременное наличие следующих условий:

- проверка ЭП оспариваемого электронного документа на Сертификате, файл которого предъявлен Банком, дала положительный результат;
- подтверждена принадлежность, актуальность и целостность Сертификата открытого ключа Клиента с помощью которого проводится проверка ЭП оспариваемого электронного поручения.

19.16. Результаты экспертизы оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения третьего этапа экспертизы. В Акте фиксируются результаты всех этапов, проведенной экспертизы, а также все существенные реквизиты оспариваемого электронного поручения. Акт составляется в двух экземплярах - по одному для представителей Банка и Клиента. Акт комиссии является окончательным и пересмотру не подлежит.

19.17. Подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ имеет юридическую силу и является законным основанием для осуществленных Банком операций по счету Клиента. Не подтверждение подлинности электронного документа, зафиксированное в Акте, будет означать, что этот документ не имеет юридической силы и не является законным основанием для осуществленных Банком операций по счету Клиента.

19.18. Акт, составленный экспертной комиссией, являются доказательством при дальнейшем разбирательстве спора в судебных органах.

19.19. При возникновении конфликтов, связанных с признанием правомочности ЭД, Стороны примут все меры к разрешению их путем переговоров .

19.20. При невозможности разрешения споров и разногласий путем переговоров они разрешаются в Арбитражном суде г. Москвы.

В ПАО «МТС-Банк»

**Заявление
о присоединении к Правилам обмена
электронными документами по Системе «Банк-Клиент»
в ПАО «МТС-Банк»**

Наименование Клиента	
ИНН	
ОГРН	
Адрес местонахождения:	
Контактная информация:	
телефон/факс	
адрес электронной почты	
комментарии	

Настоящим заявляем о присоединении _____

(наименование клиента)

к действующей редакции Правил обмена электронными документами по Системе «Банк-Клиент» в ПАО «МТС-Банк» (далее – Правила) в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации, и подтверждаем, что все положения Правил известны и разъяснены в полном объеме.

Просим предоставить доступ к Системе обмена электронными документами «Банк-Клиент» ПАО «МТС-Банк» и обеспечить возможность ее использования в соответствии с условиями Правил.

(должность Руководителя)

_____/_____
(подпись) (фамилия, имя, отчество полностью)

« 20 Г.

М.П. (при наличии)

Заполняется Банком

Заявление получено в _____ часов _____ минут « _____ » _____ г.

Работник Банка: _____

ПАО «МТС-Банк»

Приложение № 2 к Правилам обмена электронными документами по Системе «Клиент-Банк»

Акт
приема-передачи

г. Москва

«__» _____ 20__ г.

(полное наименование клиента)

далее именуемое – Клиент, в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____,

(название документа)

и Публичное акционерное общество «МТС-Банк», далее именуемый Банк, в лице _____,

(должность, фамилия, имя, отчество)

действующего на основании _____,

(название документа)

далее по тексту – Стороны, составили настоящий Акт о нижеследующем:

1.Клиенту подготовлено и предоставлено следующее программное обеспечение, переданы программно-аппаратные средства и документация (Таблица 1). Запуск программного обеспечения Клиентской части системы «Клиент-Банк» в эксплуатацию будет произведен после подписания настоящего Акта и предоставления его в Банк.

Таблица 1

Программное обеспечение			
№	Наименование	Версия	Серийный номер лицензии/ключ активации
1	Дистрибутив ПО СКЗИ Крипто-Про CSP	4.0	
2	Драйвер необходимый для работы USB-token		-
Проведение дополнительных работ			
№	Наименование	Отметка о выполнении с указанием исполнителя и даты	
1			
2			
Перечень программно-аппаратных средств и документов, переданных Клиенту			
№	Наименование		
1	USB-token ID номер носителя:		
2	Руководство пользователя системы «Клиент-Банк»		
3	Инструкция по настройке СКЗИ и изготовлению сертификатов ключей ЭП		
4	Файл объектных идентификаторов OID'S (для обозначения области применения сертификатов ключей ЭП)		
5	Комплект эксплуатационной документации СКЗИ «КриптоПро CSP»		
6	Файл корневого сертификата Удостоверяющего центра Банка		

2.Клиент ознакомлен с техническим описанием программного обеспечения, предупрежден о степени его надежности, ознакомлен и получил все документы, указанные в настоящем акте и обязуется целиком и полностью их выполнять.

3.Клиент не имеет к Банку претензий по качеству, количеству и комплектности переданных документов и программно-аппаратных средств.

ПАО «МТС-Банк»

4. Клиент предупрежден, что Банк, другие поставщики и разработчики Системы «Клиент-Банк» не гарантируют надлежащей и качественной работы программного комплекса, и не несут никакой ответственности при самостоятельной переустановке Клиентом программных средств, не соблюдении мер безопасности при работе и хранении ключевых носителей, и всех прочих событиях, нарушающих нормальное функционирование вышеуказанного программного обеспечения.

Клиент обязуется эксплуатировать СКЗИ в помещении, отвечающем техническим требованиям, изложенным в разделе № 4 Правил обмена электронными документами по системе «Клиент-Банк» в ПАО «МТС-Банк».

Административно-технические данные приведены в Таблице 2.

Таблица 2

Фактический адрес	
Адрес для корреспонденции	
Телефонный номер для экстренной связи с администратором безопасности/оператором	
Наименование подразделения, где установлен программный комплекс	
Реквизиты помещения, где установлен программный комплекс и предполагается хранить ключевые носители	

5. Стоимость подключения системы «Клиент-Банк» составляет _____ (_____) рублей ____ коп.

6. Настоящий акт составлен в двух экземплярах, по одному – для каждой из Сторон, и является неотъемлемой частью Правил обмена электронными документами по системе «Клиент-Банк» в ПАО «МТС-Банк».

Банк

Клиент

(_____) _____ (_____) _____

м.п.

м.п. (при наличии)

Приложение №3 к Правилам обмена электронными документами по системе «Клиент-Банк»

РАСПИСКА

Я, _____
(Ф.И.О.)

(должность, наименование клиента)

получил(а) в ПАО «МТС-Банк» на руки следующее программное обеспечение и документы:

- Конверт с логином и паролем для подсистемы «Интернет-Клиент» – 1 экз;
- Ключевой(ые) носитель(и) USB-token – «___» шт., для следующих пользователей:

№ п/п	Фамилия, имя, отчество (полностью)	Должность	id USB-Token
1			
2			
3			
4			

_____ (_____)

«___» _____ «201820__» года

Банк

Клиент

_____ (_____)
м.п.

_____ (_____)
м.п. (при наличии)

Место нахождения Удостоверяющего Центра ПАО «МТС-Банк»: 117545, г. Москва, 1-й Дорожный проезд, д. 3с2

Подписанный и заверенный печатью бланк сертификата открытого ключа следует передать в офис Банка по месту Вашего обслуживания

Банк

Клиент

_____ (_____)

м.п.

_____ (_____)

м.п. (при наличии)

В ПАО «МТС-Банк»

**Заявление
на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего Центра ПАО
«МТС-Банк»**

(наименование клиента)

ВЛИЩЕ _____
(должность руководителя)

(фамилия, имя, отчество)

действующего на основании _____

Просит аннулировать (отозвать) с «__» _____ 20__ г. сертификат ключа подписи своего уполномоченного представителя – Пользователя Удостоверяющего Центра ПАО «МТС-Банк», содержащий следующие идентификационные данные:

Серийный номер сертификата (SN)	
Фамилия, Имя, Отчество (CN)	
Наименование клиента (O)	

В СВЕДЕНИИ С _____
(причина отзыва сертификата *)

и выдать маркер временного доступа для перевыпуска сертификата (отметить, если нужно)

 Должность руководителя

 /

 Подпись Ф.И.О

М.П. (при наличии)

* – прекращение работы Пользователя Удостоверяющего Центра, компрометация закрытого ключа подписи и т.д.;

Приложение № 6 к Правилам обмена электронными документами по системе «Клиент-Банк»

В ПАО «МТС-Банк»

**ЗАЯВКА
на установление ограничения на подключение к электронной системе «Клиент-Банк» по сетевым адресам.**

Настоящей Заявкой

(наименование клиента)

в лице

_____ действующего на основании _____ в целях увеличения безопасности работы со своими средствами в банке, выражает намерение установить ограничение на доступ своей учетной записи в систему Клиент-банк для всех подключений, кроме производимые из сетей указанных ниже:

Интернет сотовых операторов	☐ МТС	☐ Билайн	☐ Мегафон	☐ Скайлинк
Беспроводной интернет	☐ Комстар	☐ Билайн	☐ Yota	
Любой другой провайдер интернета	Укажите диапазон IP адресов (только цифры): _____			

* Возможно одновременное указание нескольких полей.

Руководитель (должность)

Ф.И.О.

Подпись

М.П. (при наличии)

« ____ » _____ 20 __ г.

Приложение № 7 к Правилам обмена электронными документами по системе «Клиент-Банк»

В ПАО «МТС-Банк»

**ЗАЯВКА
на подключение к электронной системе «Клиент-Банк» со встроенными сертифицированными
средствами криптографической защиты информации**

Настоящей Заявкой

(наименование клиента)

в лице

действующего на основании _____ выражает намерение использовать электронную систему «Клиент-Банк» (далее по тексту – Система) для управления своим счетом (счетами).

Оборудование и помещения, предназначенные для установки программного обеспечения Системы, удовлетворяют техническим требованиям, изложенным в п.4. Правил обмена электронными документами по системе «Клиент-Банк» в ПАО «МТС-Банк».

Оплату стоимости подключения системы «Клиент-Банк», своевременную оплату абонентской платы гарантируем.

Сведения о владельцах ключей ЭП (и шифрования) и их права:

№ п/п	Фамилия, имя, отчество (полностью)	Должность и Электронная почта	Право первой подписи	Право второй подписи	Право просмотра
1			☐	☐	☐
2			☐	☐	☐
3			☐	☐	☐
4			☐	☐	☐

Ответственные лица (Ф.И.О., должность, телефон, факс, адрес электронной почты, паспортные данные):

по техническим вопросам:

по вопросам обмена информацией (не менее двух человек):

1) _____

2) _____

Адрес подключения программного обеспечения _____

Местонахождение Клиента:

ИНН _____ ОКВЭД _____ ОКПО _____
Номер банковского счета в валюте Российской Федерации: _____
в Банке _____
К/С _____ БИК _____

Руководитель (должность)

Ф.И.О.

Подпись

М.П.(при наличии)

« ____ » _____ 20 ____ г.

Отметка Банка:

Настоящим подтверждаю, что сведения, указанные в ЗАЯВКЕ проверены « ____ » _____ 20 ____ г.

Должность уполномоченного представителя Банка
Ф.И.О.

_____ / _____ /
Подпись

Приложение № 7а к Правилам обмена электронными документами по системе «Клиент-Банк»

В ПАО «МТС-Банк»

**ЗАЯВКА
на подключение к электронной системе «Клиент-Банк» со встроенными сертифицированными
средствами криптографической защиты информации**

Настоящей Заявкой _____

(наименование клиента)

в лице _____
действующего на основании _____ выражает намерение использовать
электронную систему «Клиент-Банк» (далее по тексту – Система) для управления своим счетом (счетами).

Оборудование и помещения, предназначенные для установки программного обеспечения Системы,
удовлетворяют техническим требованиям, изложенным в п.4. Правил обмена электронными документами по
системе «Клиент-Банк» в ПАО «МТС-Банк».

Оплату стоимости подключения системы «Клиент-Банк», своевременную оплату абонентской платы
гарантируем.

Сведения о владельцах ключей ЭП (и шифрования) и их права:

№ п/п	Фамилия, имя, отчество (полностью)	Должность	Адрес электронной почты	Право акцепта
1				☐
2				☐
3				☐
4				☐

Ответственные лица (Ф.И.О., должность, телефон, факс, адрес электронной почты, паспортные данные):
по техническим вопросам:

по вопросам обмена информацией (не менее двух человек):

1) _____

2) _____

Адрес подключения программного обеспечения _____

Местонахождение Клиента:

ИНН _____ ОКВЭД _____ ОКПО _____

Номер банковского счета в валюте Российской Федерации: _____

в Банке _____

К/С _____ БИК _____

Руководитель (должность) _____ Ф.И.О. _____ Подпись _____

М.П.(при наличии)

« ____ » _____ 20 __ г.

Отметка Банка:

Настоящим подтверждаю, что сведения, указанные в ЗАЯВКЕ проверены «__» _____ г.

_____/_____
Должность уполномоченного представителя Банка Подпись Ф.И.О.

Приложение № 8 к Правилам обмена электронными документами по системе «Клиент-Банк»

**Заявление на регистрацию Пользователя
в Удостоверяющем центре ПАО «МТС-Банк»**

_____ (полное наименование клиента, включая организационно-правовую форму)
в лице _____,
_____ (должность, фамилия, имя, отчество)
действующего на основании _____
Просит зарегистрировать уполномоченного представителя

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

в Реестре Удостоверяющего центра и изготовить сертификат открытого ключа подписи (и шифрования) в соответствии со следующими идентификационными данными и областями использования ключа:

Фамилия, Имя, Отчество (CN)		
Наименование клиента (O)		
Населенный пункт (L)		
Регион (край/область) (S)		
Страна (C)		
Адрес электронной почты (E)		
Extended Key Usage	Защищенная электронная почта, Подписывание документа Клиент системы Клиент-Банк Пользователь Центра Регистрации, HTTP, TLS клиент Проверка подлинности клиента	(1.3.6.1.5.5.7.3.4) (1.3.6.1.4.1.311.10.3.12) (1.2.643.4.16.2.2) (1.2.643.2.2.34.6) (1.3.6.1.5.5.7.3.2)

Средство электронной цифровой подписи: СКЗИ «КриптоПро CSP» Алгоритм: ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012.

Настоящим подтверждаю, что присоединяюсь к Регламенту Удостоверяющего Центра ПАО «МТС-Банк», и обязуюсь соблюдать все положения указанного документа, а так же соглашаюсь с обработкой своих персональных данных Удостоверяющим Центром и признаю, что персональные данные, включенные в сертификат ключа подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным:

Уполномоченный представитель клиента,
регистрирующийся в Удостоверяющем центре _____ / _____ /
«___» _____ 20___ г.
_____ М.П.(при наличии) / _____ /
Должность руководителя Подпись Ф.И.О.

Настоящим подтверждаю, что Заявление о регистрации _____
_____ в Реестре
Удостоверяющего центра ПАО «МТС-Банк» получено, личность идентифицирована, сведения,
указанные в Заявлении, проверены. «___» _____ 20___ г.

_____ / _____ /
Должность уполномоченного представителя Банка Подпись Ф.И.О.

Наименование Клиента	
ИНН	
ОГРН	
Контактная информация:	
телефон/факс	
адрес электронной почты	
комментарии	

Настоящим заявляем о расторжении с «_____» _____ 20__ г. договора об обмене электронными документами по Системе «Банк-Клиент», заключенного путем присоединения к условиям Правил обмена электронными документами по Системе «Банк-Клиент» в ПАО «МТС-Банк» на основании Заявления от «_____» _____ 20__ г.

(должность Руководителя)

_____/_____/_____
(подпись) (фамилия, имя, отчество полностью)

« » 20 г.

М.П.(при наличии)

Заполняется Банком

Заявление получено в _____ часов _____ минут « _____ » _____ г.

Работник Банка: _____

подпись

Фамилия И.О.

ПАО «МТС-Банк»